User Manual

Gateway U270V

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router are used in a normal manner with a well-constructed network, the router should not be used in situations where failure to transmit or receive data could result indamage of any kind to the user or any other party, including but not limited to personal injury, death or loss of property. Atel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Atel router or for failure of the Atel router to transmit or receive such data.

Safety Precautions

Do not operate the router:

- In areas where blasting is in progress
- Where explosive atmospheres may be present
- Near medical equipment
- Near life support equipment or any equipment that may be susceptible to any form of radio interference. In such areas, the router MUST BE POWERED OFF. The Atel router can transmit signals that could interfere with this equipment.

Do not operate the router in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the router MUST BE POWERED OFF. When operating, the router can transmit signals that could interfere with various onboard systems.

☞ **Note:**

Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. The router may be used at this time.

The driver or operator of any vehicle should not operate the router while in control of a vehicle. Doing so will detract from the driver or operator’s control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offense.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Atel.

ATEL SPECIFICALLY DISCLAIMS LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANYATEL PRODUCT, EVEN IF ATEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

TABLE OF CONTENTS

1. Introduction

Thank you for purchasing the U270V router with Voice over IP (VoIP). This user manual will help you setup, configure and outline best practices for maximizing your home network performance with the router.

2. Product Overview

In minutes, you will be able to connect your computers to the Internet and you will be able to make a phone call using VoIP. The following is a list of features that make your new U270V router an ideal solution for your home or small office network. Implementation of these features depends on the particular service provider and account features you have chosen.
Some features described in this manual may not be supported by your service provider or may not be available with your network account. For details of the services and accounts available, contact your service provider.

VoIP Calling
Your router (U270V) features a Voice over Internet Protocol (VoIP) function that allows you to make voice calls over a VoIP network by simply connecting a wired, landline phone to your network-connected router.

Plug-and-Play
Your router was factory-set for compatibility with a particular service provider. Thus, your router operates on radio channels and enables services specific to your network service provider. Once your router has been activated on your service provider's network, you can connect to the Internet. After your router is activated, connect it to your computer using the Ethernet (RJ-45) cable or via Wi-Fi. You are now ready to use the Internet.

Web-Based Advanced User Interface
You can easily setup the router's advanced functions through your web browser and without having to install additional software onto your computer. There are no drivers to install and, you can easily make changes and perform setup functions from any computer that is connected to your U270V

- NAT IP Address Sharing
- Support for VPN Pass Through
- Built in Dynamic Host Configuration Protocol (DHCP)
- Integrated 802.11b/g/n Wireless Access Point
- MAC Address Filtering

Integrated 10/100 Mbit/s 3-Port Switch
The U270V has a built-in 3-port network switch to allow your wired computers to share printers, data and MP3files, digital photos, and much more. The switch features automatic detection so it will adjust to the speed of connected devices. The switch will transfer data between computers and the Internet simultaneously without interrupting or consuming resources.

Integrated 802.11 b/g/n Wireless Access Point

The U270V supports Wi-Fi modes b/g and n. Your router as default is set to Wi-Fi b/g/n mixed mode. To use another mode you can change this by logging into the web interface (instructions can be found in section 4.4.1.2).

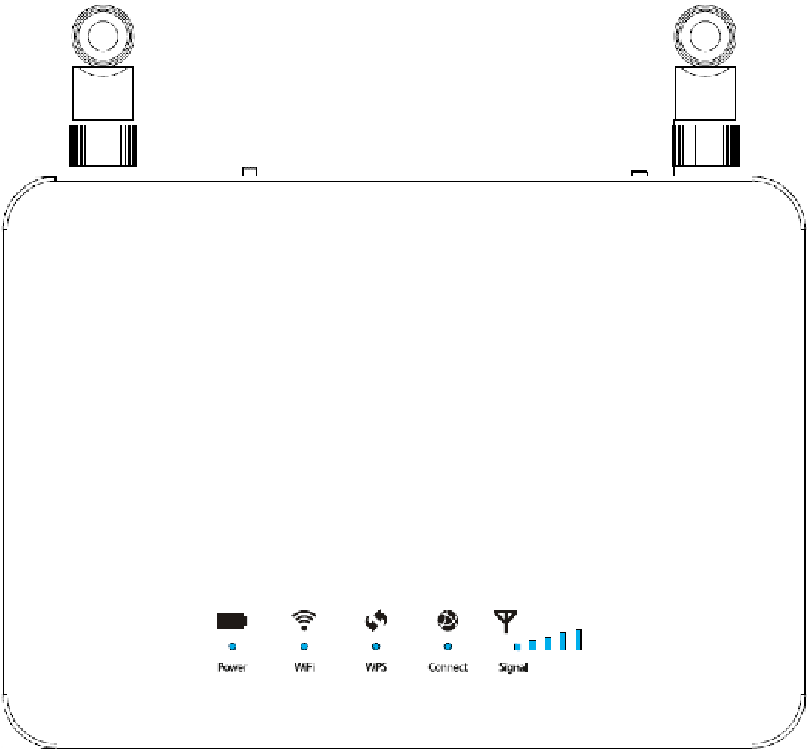
3. Using your Router

3.1 Package Contents

- U270V router
- 2xAntennas
- RJ-45 Ethernet Networking Cable
- Power Supply and Car Charger (12V)
- Quick guide

3.2 Router Interfaces

The U270V is designed to be placed on a desktop or wall mounted. All the ports at the back of the router are for better organization and utility. The LED indicators are easily visible on the top of the router to provide you with information about network activity and status.



3.3 LED

Items	Description

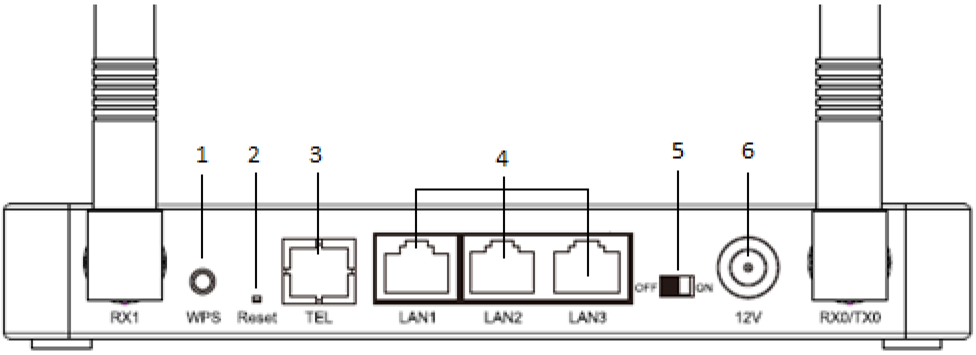
Power	On(Yellow)	Only charger plug or Full charged
	Blinking(Yellow)	Charger plug in and charge for battery
	Blinking (Red)	Battery in and no charger plug in the battery is in low status,
WIFI	On(Yellow)	WIFI has turned on
	Blinking(Yellow)	Active data passed through Wi-Fi
	OFF	WIFI has turned off
WPS	Blinking(Yellow)	WPS is activated. WPS led is off after one minutes
	Off	WPS is Off
Connect	On(Yellow)	LTE data connection is established
	Blinking(Yellow)	LTE data is connecting
	Off	No data connection
Signal	On(Yellow)	Band 31
	On(Green)	Band 3
	On(pink)	Band 7
	On(Blue)	Band 20

3.4 RJ-45 Switch

The RJ-45 Switch has three Ethernet ports supporting up to 100 Mbit/s. Use any of the 3 ports and an Ethernet cable to connect the router to your computer.

3.5 Other Features

（1）WPS Key
（2）Reset Key
（3）Phone line（RJ-11）
（4）Network connection to Computers (RJ-45/Ethernet)
（5）Power On/Off Switch
（6）Power Jack



3.6 Setting up your hardware

1. Make sure your router is not connected to any power source and that all the LEDs are OFF.
2. How to setup the antennas for maximized performance:

①Antennas are located on both sides of the router.

②Attach the antennas to the back of the router

③Hand tighten the antennas so that they are securely attached to the router

3. Locate the power supply that is included with your router. Plug the power supply's small connector into the power port on the router (6). Plug the power supply into an empty power outlet.
4. Switch on the router (5). Look at the Power LED on top of the router and make sure the LED is lit.
5. Wait for a few seconds while the router searches for network service. When the router finds

a suitable network the Connect LED is lit yellow. Refer to the Signal LED's for acquired signal strength and band.

6. Locate the Ethernet cable that is included with your router. Plug one end of the cable into any Ethernet port on your router. Plug the other end of the cable into the networking port on your computer.
   Alternatively connect to the router through Wi-Fi

4. Configuring the router

The following section will guide you through the steps to properly configure and personalize all settings in your router.

4.1 Login

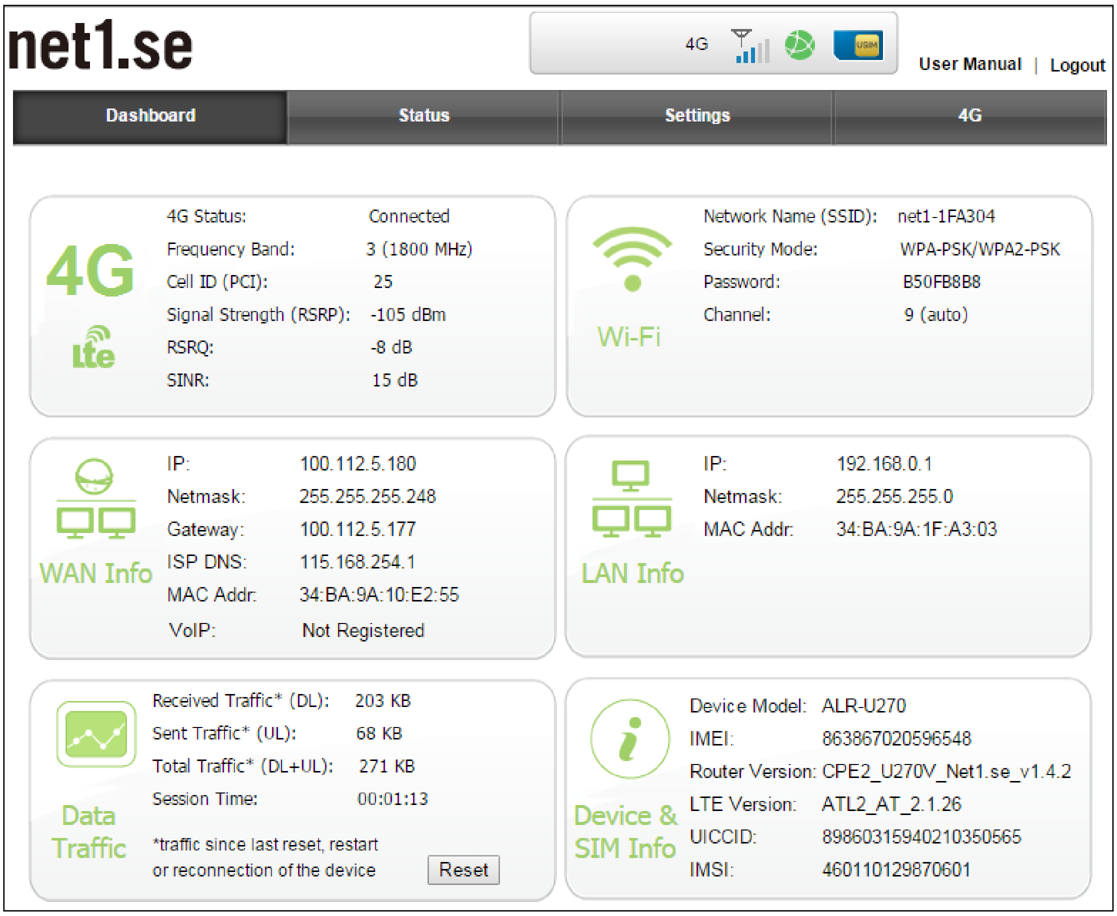
Open a web browser and enter 192.168.0.1 in the address bar. A login window will be displayed and you will be prompted to enter a username and a password to login.

Use the following information to login:
Username: admin
Password: admin

When successfully logged in you will be able to navigate through the web interface of the router. The web interface persists of four main section called Dashboard, Status, Settings and 4G. Every section has their own submenus with pages to display more specific information or options for that particular subject or feature.

4.2 Dashboard

On the dashboard you will have a view over the most important information the web interface can provide including radio parameters, WAN and LAN IP addresses, Wi-Fi SSID and password, software versions and SIM identification numbers and at the top you can find SIM status, connection status as well as a hyperlink to Net1 support webpage and the logout button.



4G Status: Connected
Frequency Band: 3 (1800 MHz)
Cell ID (PCI): 25
Signal Strength (RSRP): -105 dBm
RSRQ: -8 dB
SINR: 15 dB

Network Name (SSID): net1-1FA304
Security Mode: WPA-PSK/WPA2-PSK
Password: B50FB8B8
Channel: 9 (auto)

IP: 100.112.5.180
Netmask: 255.255.255.248
Gateway: 100.112.5.177
ISP DNS: 115.168.254.1
MAC Addr: 34:BA:9A:10:E2:55
VoIP: Not Registered

IP: 192.168.0.1
Netmask: 255.255.255.0
MAC Addr: 34:BA:9A:1F:A3:03

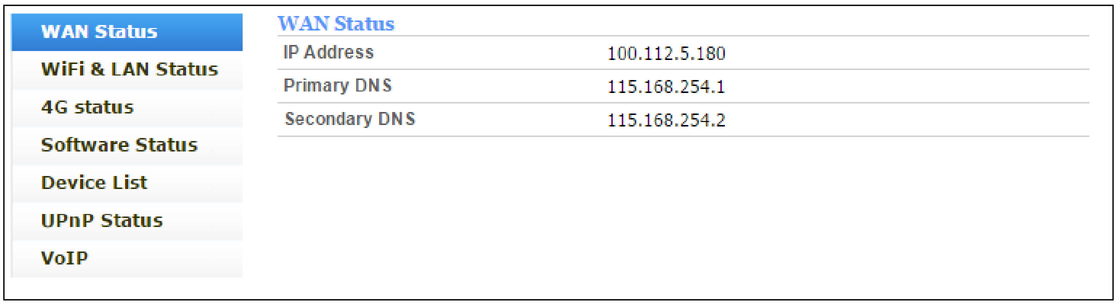
Received Traffic* (DL): 203 KB
Sent Traffic* (UL): 68 KB
Total Traffic* (DL+UL): 271 KB
Session Time: 00:01:13
*traffic since last reset, restart or reconnection of the device

Device Model: ALR-U270
IMEI: 863867020596548
Router Version: CPE2_U270V_Net1.se_v1.4.2
LTE Version: ATL2_AT_2.1.26
UICCID: 89860315940210350565
IMSI: 460110129870601

Figure 4-2-1Dashboard Page

4.3 Status

In this section you will find the status pages for Wi-Fi & LAN, 4G, Software versions, Device List, UPnP and VoIP.



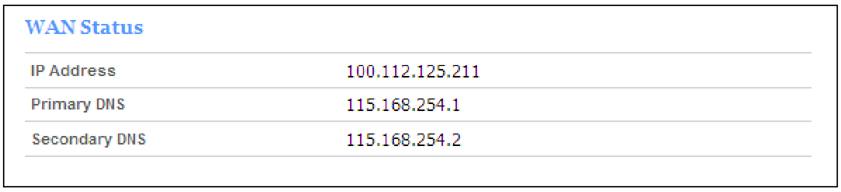
WAN Status

IP Address	100.112.5.180
Primary DNS	115.168.254.1
Secondary DNS	115.168.254.2

Figure 4-3-1 Status

4.3.1 WAN Status

On the WAN Status page you can see WAN IP Address, WAN Primary DNS and WAN Secondary DNS information.



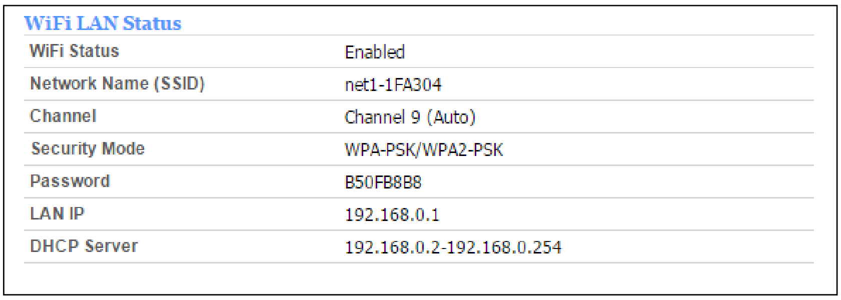
WAN Status

IP Address	100.112.125.211
Primary DNS	115.168.254.1
Secondary DNS	115.168.254.2

Figure4-3-1-1 WAN Status

4.3.2 WiFi & LAN Status

On this page you can see Wi-Fi & LAN information such as SSID, Channel, Security mode, LAN IP and DHCP Server information.



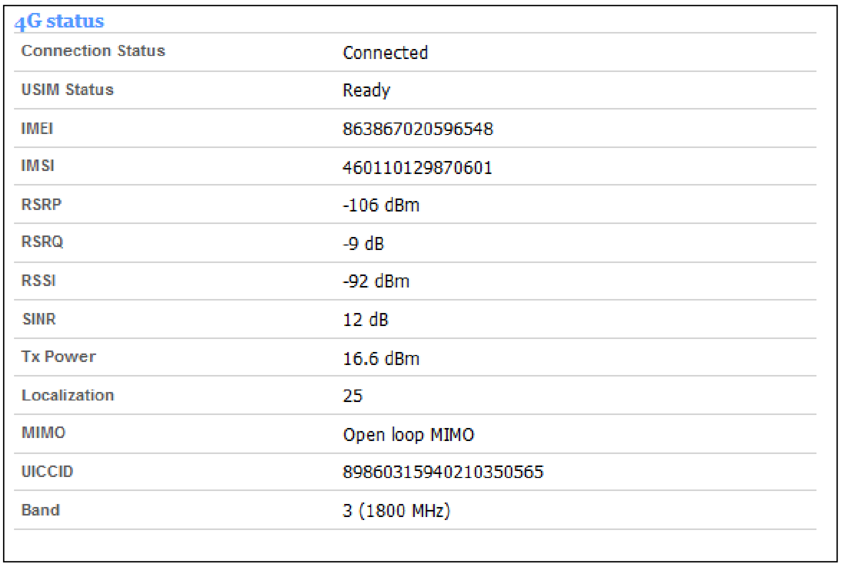
WiFi LAN Status

WiFi Status	Enabled
Network Name (SSID)	net1-1FA304
Channel	Channel 9 (Auto)
Security Mode	WPA-PSK/WPA2-PSK
Password	B50FB8B8
LAN IP	192.168.0.1
DHCP Server	192.168.0.2-192.168.0.254

Figure 4-3-2-1 WiFi LAN Status

4.3.3 4G Status

In the 4G Status menu you can see LTE information like Connection Status, SIM Status, SIM numbers, Radio levels, MIMO status and frequency of the LTE network you are connected to.



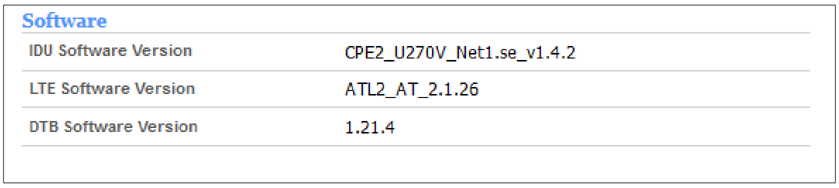
4G status

Connection Status	Connected
USIM Status	Ready
IMEI	863867020596548
IMSI	460110129870601
RSRP	-106 dBm
RSRQ	-9 dB
RSSI	-92 dBm
SINR	12 dB
Tx Power	16.6 dBm
Localization	25
MIMO	Open loop MIMO
UICCID	89860315940210350565
Band	3 (1800 MHz)

Figure 4-3-3-1 LTE Status

4.3.4 Software Status

On this page you can see installed IDU- and LTE software versions.



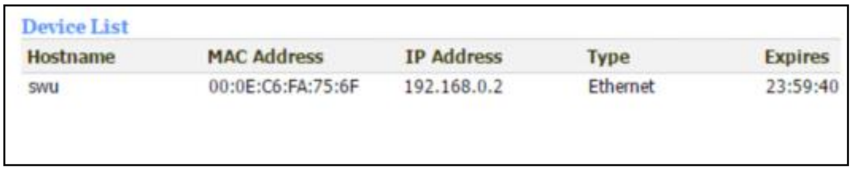
Software

IDU Software Version	CPE2_U270V_Net1.se_v1.4.2
LTE Software Version	ATL2_AT_2.1.26
DTB Software Version	1.21.4

Figure 4-3-4-1 Software

4.3.5 Device List

In the device list you can see information regarding currently connected devices like hostname, MAC address, IP address, expiring time and connection type.



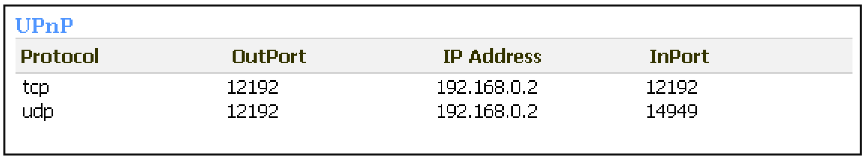
Device List

Hostname	MAC Address	IP Address	Type	Expires
swu	00:0E:C6:FA:75:6F	192.168.0.2	Ethernet	23:59:40

Figure 4-3-5-1 Device List

4.3.6 UPnP Status

On the UPnP Status page you can see rules for active UPnP connections.



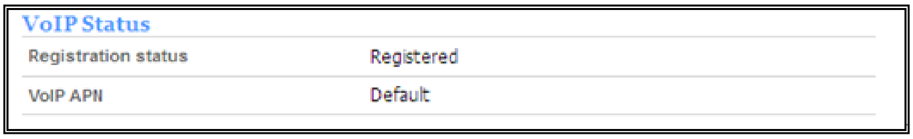
UPnP

Protocol	OutPort	IP Address	InPort
tcp	12192	192.168.0.2	12192
udp	12192	192.168.0.2	14949

Figure 4-3-6-1 UPnP

4.3.7 VoIP

The VoIP page displays Registration status and VoIP APN.



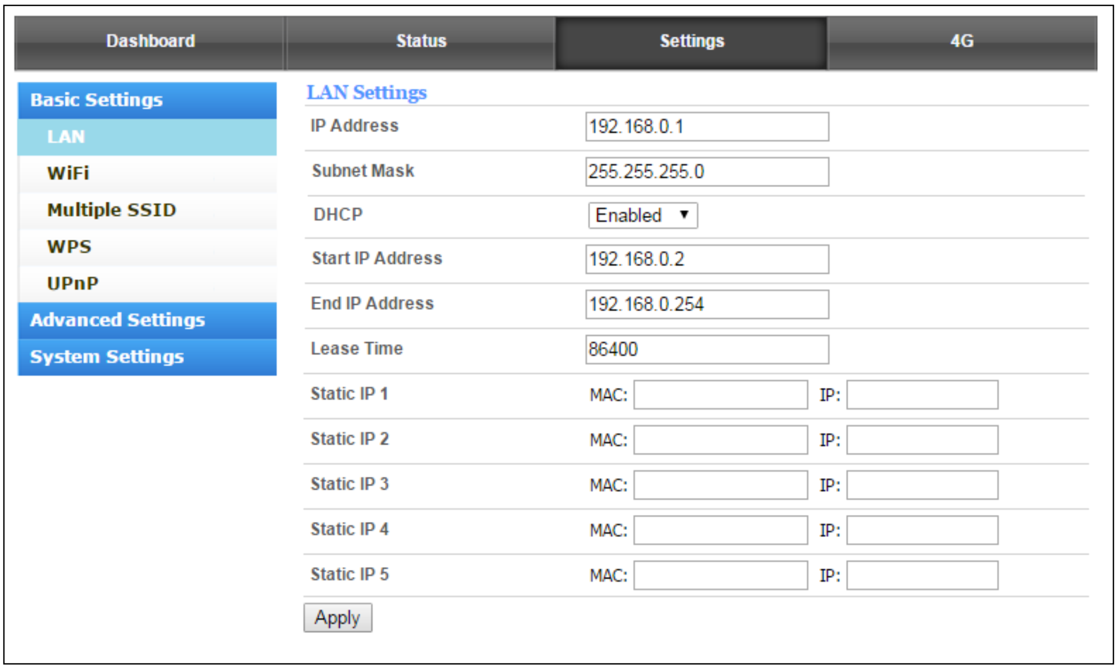
VoIP Status

Registration status	Registered
VoIP APN	Default

Figure 4-3-7-1 VoIP

4.4 Settings

The Settings section consists of three main menus named Basic Settings, Advanced Settings and System Settings.

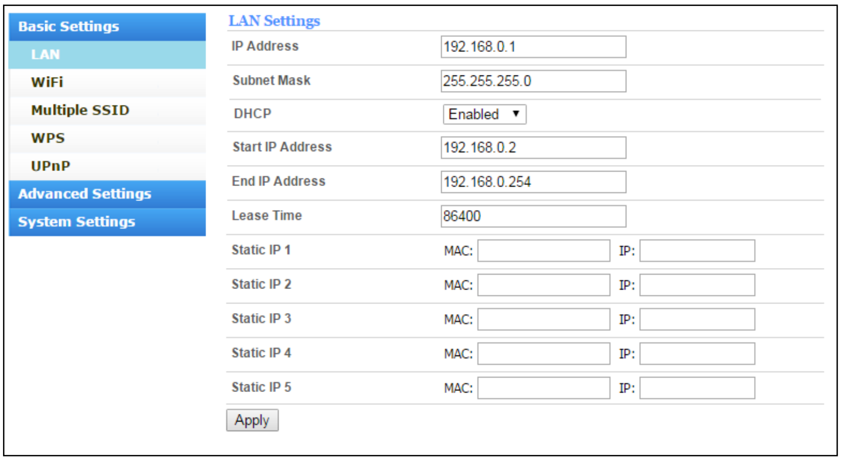


LAN Settings

IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP: Enabled
Start IP Address: 192.168.0.2
End IP Address: 192.168.0.254
Lease Time: 86400
Static IP 1 MAC: IP:
Static IP 2 MAC: IP:
Static IP 3 MAC: IP:
Static IP 4 MAC: IP:
Static IP 5 MAC: IP:

Figure4-4-1 Settings

4.4.1 Basic Settings



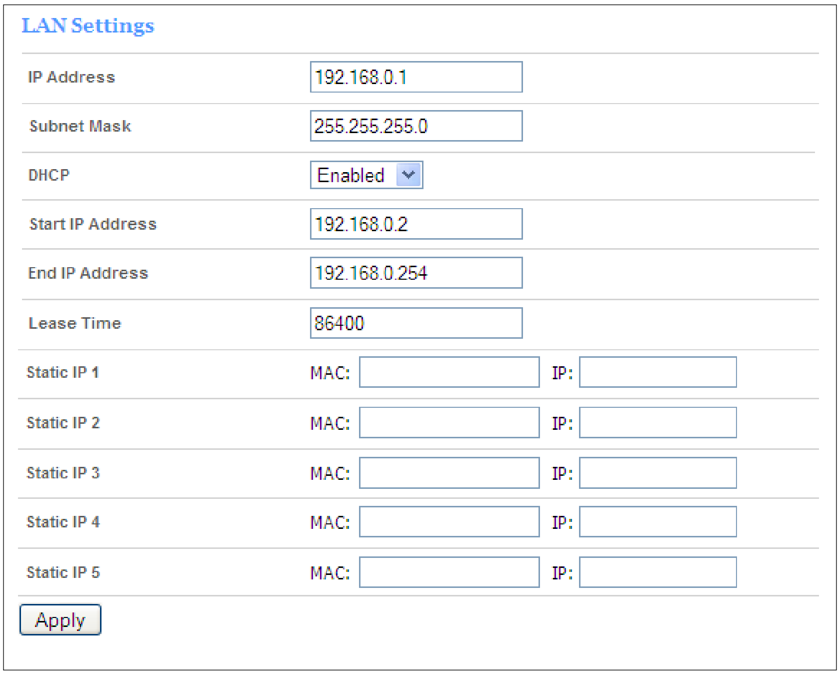
LAN Settings

IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP: Enabled
Start IP Address: 192.168.0.2
End IP Address: 192.168.0.254
Lease Time: 86400
Static IP 1 MAC: IP:
Static IP 2 MAC: IP:
Static IP 3 MAC: IP:
Static IP 4 MAC: IP:
Static IP 5 MAC: IP:

Figure4-4-1-1 Basic Settings

4.4.1.1 LAN Settings

On the LAN Settings page all settings for the internal LAN can be viewed and changed.



LAN Settings

IP Address	192.168.0.1	
Subnet Mask	255.255.255.0	
DHCP	Enabled	
Start IP Address	192.168.0.2	
End IP Address	192.168.0.254	
Lease Time	86400	
Static IP 1	MAC:	IP:
Static IP 2	MAC:	IP:
Static IP 3	MAC:	IP:
Static IP 4	MAC:	IP:
Static IP 5	MAC:	IP:

Figure 4-4-1-1-1 LAN Settings

- **IP Address**

  Enter the IP address of your router (factory default: 192.168.0.1).

- **Subnet Mask**

  Subnet mask is an address code that determines the size of a network. The subnet mask is by default set to 255.255.255.0 (/24) and cannot be changed.

- **DHCP**

  Enables or Disables the DHCP server. If you disable the DHCP server, you must have another DHCP server within your network or you will have to configure static IP addresses on all other devices.

- **Start IP Address**

  Specifies an IP address for the DHCP server to start with when assigning IP addresses to hosts. The default starting address is 192.168.0.2. This address cannot end with .0, .1 or .255 as these addresses are reserved for network, gateway and broadcast addresses.

- **End IP Address**

  Specifies an ending IP address with when assigning IP addresses to hosts. When all IP addresses are used no more devices can be connected. The default end address is 192.168.0.254. This address cannot end with .0, .1 or .255 as these addresses are reserved for network, gateway and broadcast addresses.

- **Lease Time**

Specifies the amount of time in seconds a host will keep the assigned IP address. When the lease time is up the host will be assigned a new IP address.

- **Static IP**

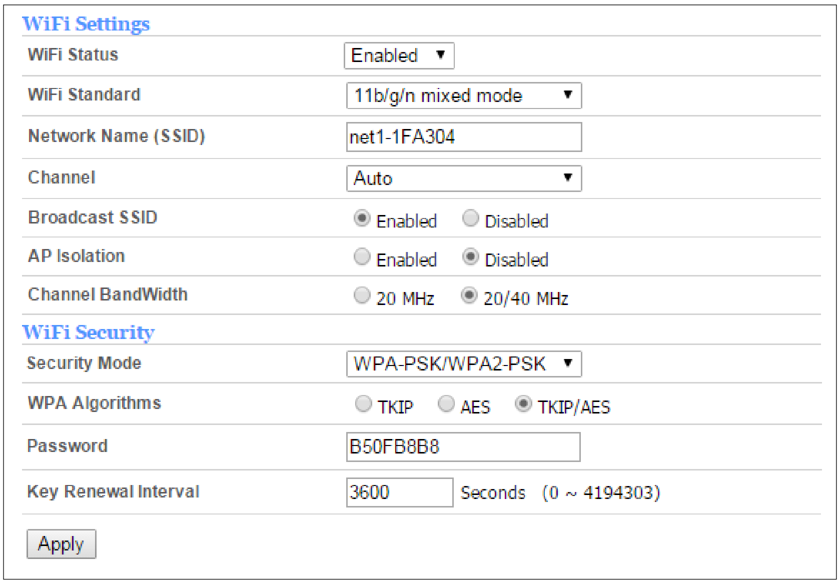
IP/MAC binding function, the router will assign a static IP address to a host with a MAC address matching with what is specified.

☞ Note:

1. If you change IP address for the router you must use the new address to access the web interface.
2. If you configure the router IP address to be in another subnet the DHCP will automatically adapt but advanced settings like port forwarding needs to be re-configured.

4.4.1.2 Wi-Fi Settings

On the Wi-Fi Settings page you can configure your Wi-Fi and WLAN to match your personal preference like changing network name and password for security reasons and change channel and bandwidth for performance optimization.



WiFi Settings	
WiFi Status	Enabled ▼
WiFi Standard	11b/g/n mixed mode ▼
Network Name (SSID)	net1-1FA304
Channel	Auto ▼
Broadcast SSID	● Enabled ○ Disabled
AP Isolation	○ Enabled ● Disabled
Channel BandWidth	○ 20 MHz ● 20/40 MHz
WiFi Security	
Security Mode	WPA-PSK/WPA2-PSK ▼
WPA Algorithms	○ TKIP ○ AES ● TKIP/AES
Password	B50FB8B8
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

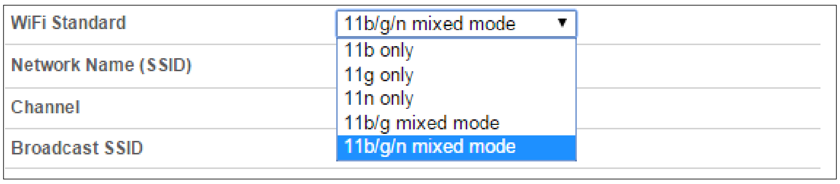
Figure 4-4-1-2-1 WiFi Settings

- **Wi-Fi Status**

The Wi-Fi status is enabled in default, you can only connect to the device by CAT-5 Ethernet cable if it is disabled.

- **Wi-Fi Standard**

The router can operate in five different wireless modes: ”11b/g mixed mode”, “11b only”, “11g only”, “11b only”, ”11b/g/n mixed mode”.



WiFi Standard: 11b/g/n mixed mode

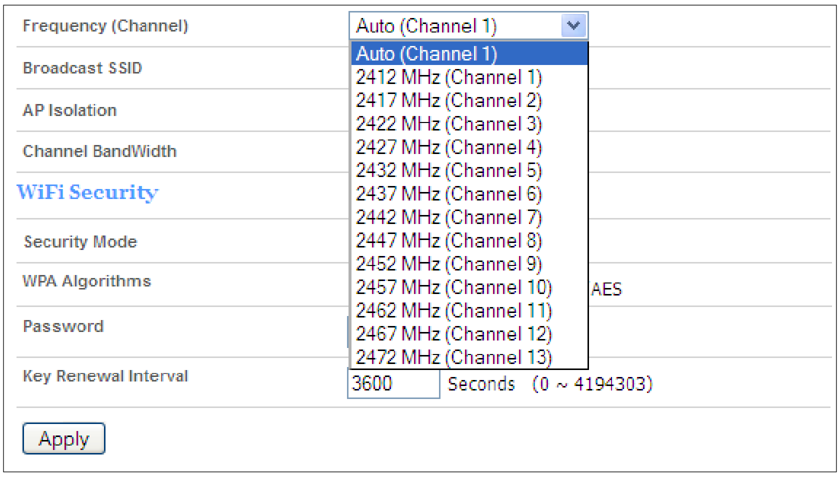
Figure 4-4-1-2-2 WiFi standard

➢ Network Name (SSID)

To identify your wireless network, a network name called SSID (Service Set Identifier) is used. You can set it to anything you like and you should make sure that your SSID is unique if there are other wireless networks operating in your area.

➢ Channel

This option determines what frequency your WLAN will be operating in. It is not necessary to change channel unless you are experiencing interference from other nearby WLANs.



Frequency (Channel): Auto (Channel 1)

WPA Algorithms: AES

Key Renewal Interval: 3600 Seconds (0 ~ 4194303)

Figure 4-4-1-2-3 Frequency (Channel)

➢ Broadcast SSID

By broadcasting the SSID local wireless devices will display the network name in its list of available WLANs. If broadcasting is disabled the SSID is “invisible” and must be entered manually by the user in the device.

➢ AP Isolation

This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other.

➢ Channel Bandwidth

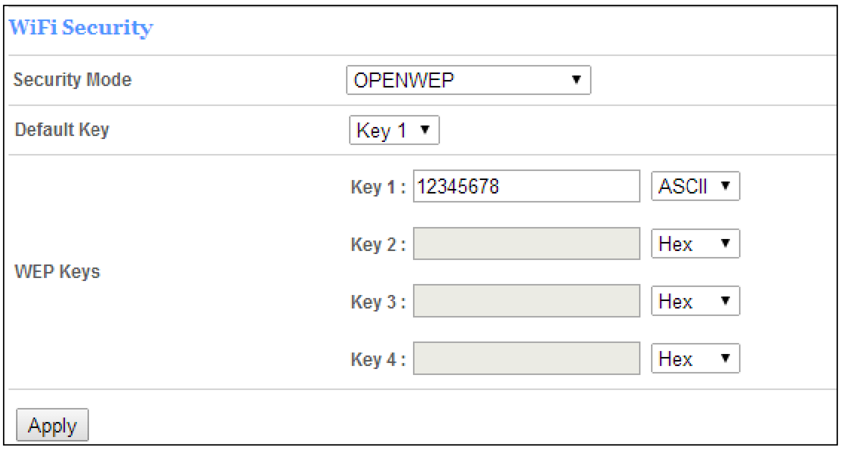
20 MHz channel bandwidth support up to150 Mbit/s connections.

40 MHz channel bandwidth support up to 300 Mbit/s connections.

➢ **Security Mode:** Disabled, OPENWEP, SHAREDWEP, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK

a) **WEP Security Mode**

- **Security Mode:** OPEN, SHARED
- **Key Format:** Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
- **Default Key:** Anyone of Key 1, Key 2, Key 3 and Key4 with 2 kinds of key format.



WiFi Security

Security Mode: OPENWEP

Default Key: Key 1

WEP Keys

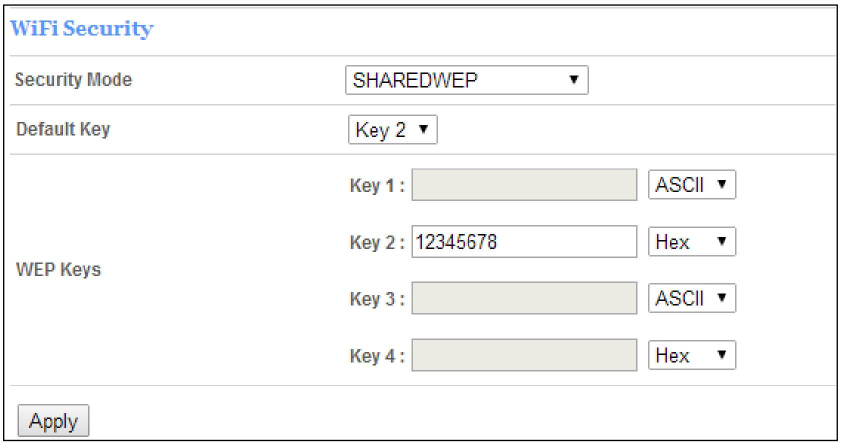
Key 1 : 12345678 ASCII

Key 2 : Hex

Key 3 : Hex

Key 4 : Hex

Figure 4-4-1-2-4 OPENWEP



WiFi Security

Security Mode: SHAREDWEP

Default Key: Key 2

WEP Keys

Key 1 : ASCII

Key 2 : 12345678 Hex

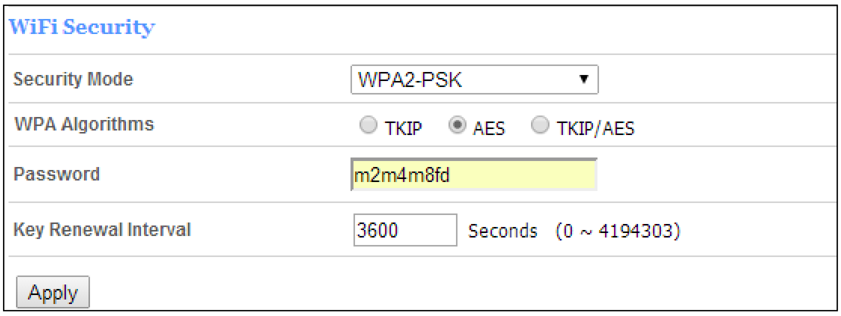
Key 3 : ASCII

Key 4 : Hex

Figure 4-4-1-2-5 SHAREDWEP

b) **WPA Security Mode**

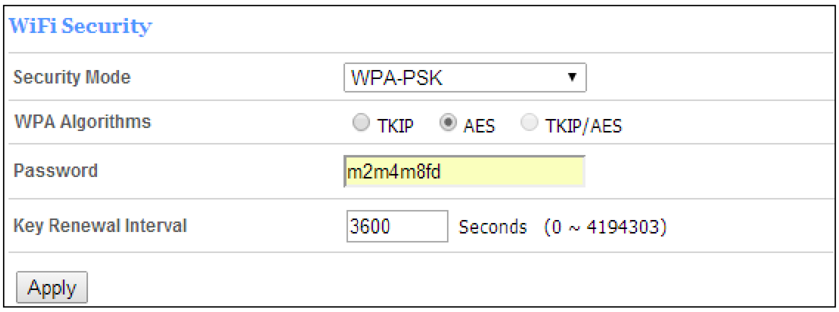
- **Security Mode:** WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK
- **WPA Algorithms:** TKIP, AES, TKIPAES
- **Keywords:** 1~32 characters
- **Key Renewal Interval:** 0~4194303s



WiFi Security

Security Mode	WPA2-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

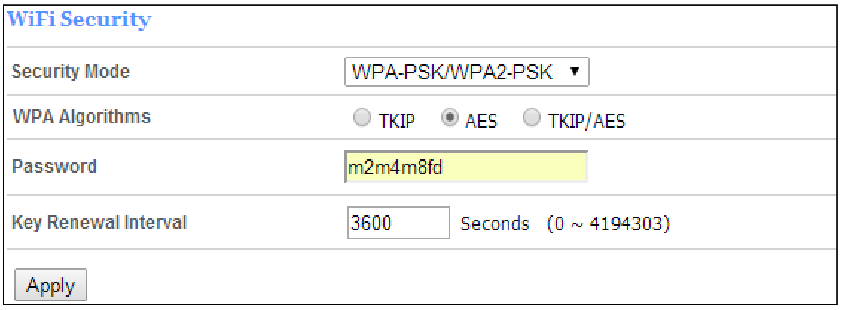
Figure 4-4-1-2-6 Default WiFi Security



WiFi Security

Security Mode	WPA-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

Figure 4-4-1-2-7 WPA-PSK



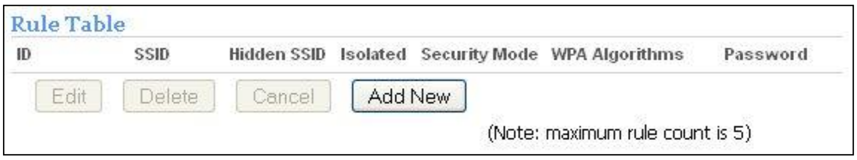
WiFi Security

Security Mode	WPA-PSK/WPA2-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

Figure 4-4-1-2-8 WPA-PSK/WPA2-PSK

4.4.1.3 Multiple SSID

On this page you can add multiple SSID's to be used when connecting to your WLAN. New SSID's will be displayed in the rule table and can be edited or deleted. Maximum rule count is 5.

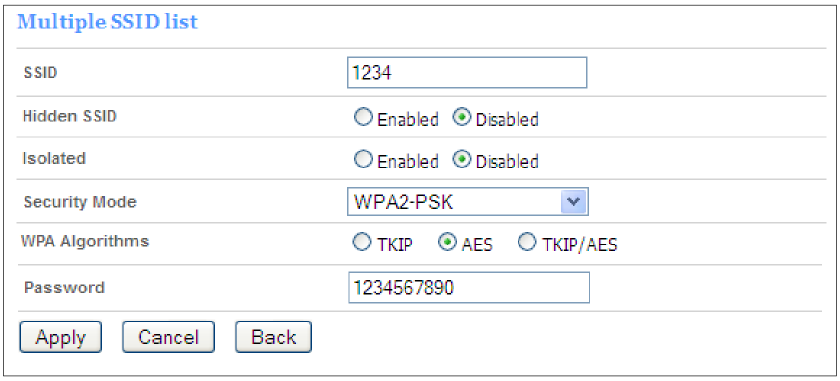


Rule Table

ID	SSID	Hidden SSID	Isolated	Security Mode	WPA Algorithms	Password

(Note: maximum rule count is 5)

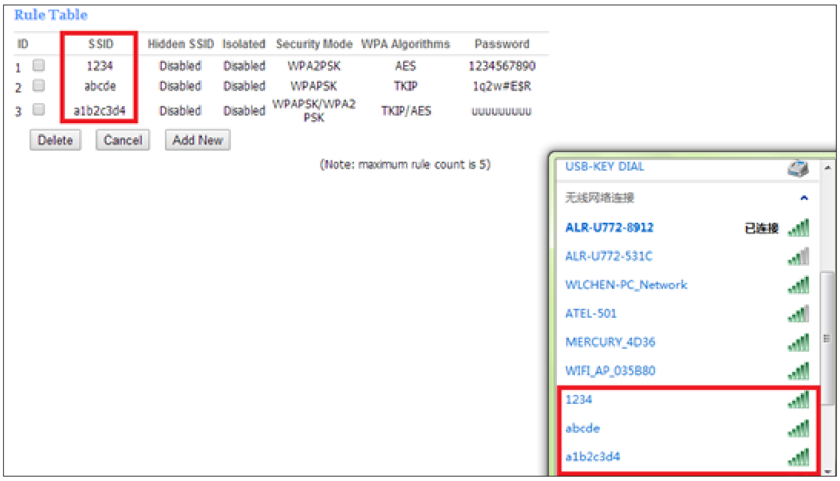
Figure 4-4-1-3-1 Multiple SSID page



Multiple SSID list

SSID	1234
Hidden SSID	○ Enabled ● Disabled
Isolated	○ Enabled ● Disabled
Security Mode	WPA2-PSK
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	1234567890

Figure 3-4-1-3-2 Add New Rule



Rule Table

ID		SSID	Hidden SSID	Isolated	Security Mode	WPA Algorithms	Password
1	□	1234	Disabled	Disabled	WPA2PSK	AES	1234567890
2	□	abcde	Disabled	Disabled	WPAPSK	TKIP	1q2w#E$R
3	□	a1b2c3d4	Disabled	Disabled	WPAPSK/WPA2 PSK	TKIP/AES	uuuuuuuuu

(Note: maximum rule count is 5)

Figure 4-4-1-3-3 Rule Table

4.4.1.4 WPS Settings

On this page, you can modify WPS settings. This feature can make your wireless client within a few minutes automatically synchronized with the WLAN and establish the connection via Wi-Fi.

- **WPS method**

  Push the button (default), Enter the PIN of client device, Use the PIN of the device.

- **WPS Status**

  This displays the real-time information of WPS processing while wireless client tries to communicate with each other over Wi-Fi.

- **PBC Mode**

  (1)Press the WPS button on your router.

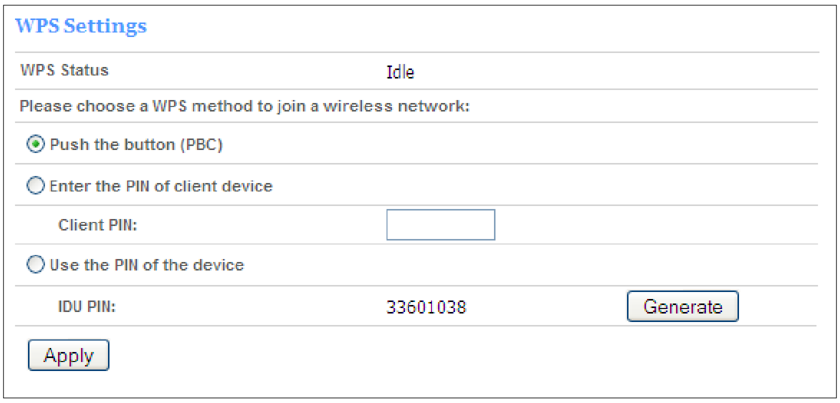
  (2)If your device is set to search for other WPS devices the router will automatically send it's WLAN information to your device over Wi-Fi and a handshake will be performed between them and your device will connect to your WLAN.

- **Enter the PIN of client device**

  (1) Wireless clients choose enrollee mode, the wireless client software will randomly generate a PIN code. Then click on the tool interface "PIN" button.
  (2) Input the PIN code which got from the wireless client and click the “Apply” button on this “WPS” configuration page.

- **Use the PIN of the device**

  (1)Create the random PIN by clicking the “Generate” button, and share this PIN to wireless client.
  (2) In the wireless client choice registrar model, and the input device of the PIN code.



WPS Settings

WPS Status Idle

Please choose a WPS method to join a wireless network:

● Push the button (PBC)

○ Enter the PIN of client device

Client PIN:

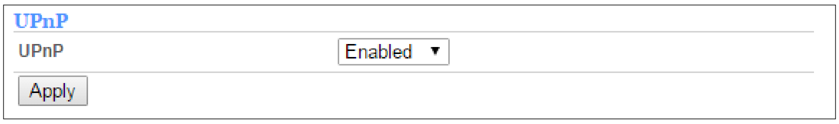
○ Use the PIN of the device

IDU PIN: 33601038

Figure 4-4-1-4-1 WPS page

4.4.1.5 UPnP

On this page you can enable or disable UPnP.

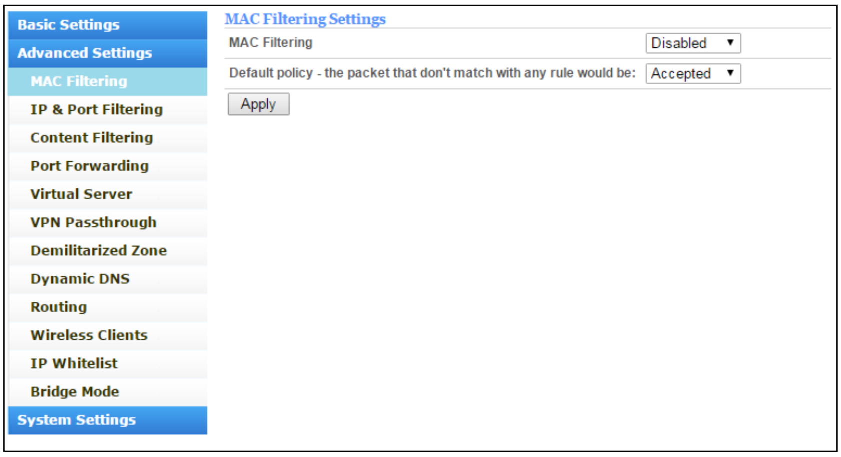


UPnP

UPnP Enabled

Figure 4-4-1-5-1 UPnP

4.4.2 Advanced Settings



MAC Filtering Settings

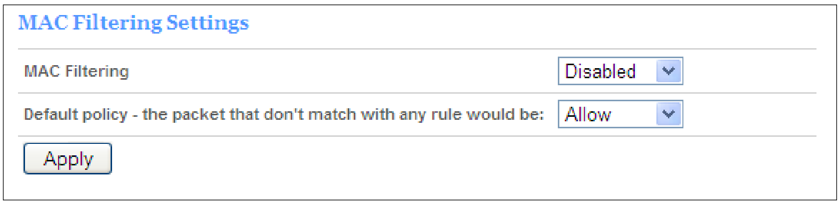
MAC Filtering: Disabled

Default policy - the packet that don't match with any rule would be: Accepted

Figure 4-4-2-1Advanced Settings

4.4.2.1 MAC Filtering

MAC filtering is a security tool that allows you to configure internet restrictions for specified devices based on MAC address. MAC filtering is disabled by default so it must be enabled before filters can be configured. If you choose the “Allowed” option for default policy, packets routed to the MAC address specified in the rules will be dropped and vice versa. In short the “Allowed” option is creating a blacklist and the “Dropped” option is creating a whitelist.

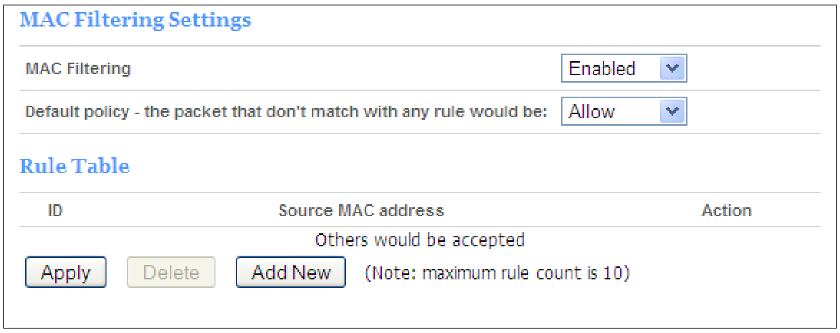


MAC Filtering Settings

MAC Filtering: Disabled

Default policy - the packet that don't match with any rule would be: Allow

Figure 4-4-2-1-1 MAC Filtering page



MAC Filtering Settings

MAC Filtering: Enabled

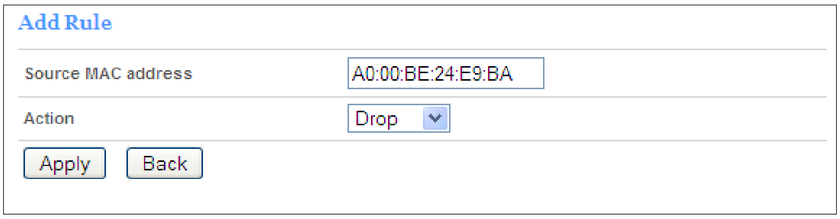
Default policy - the packet that don't match with any rule would be: Allow

Rule Table

ID	Source MAC address	Action
	Others would be accepted	

(Note: maximum rule count is 10)

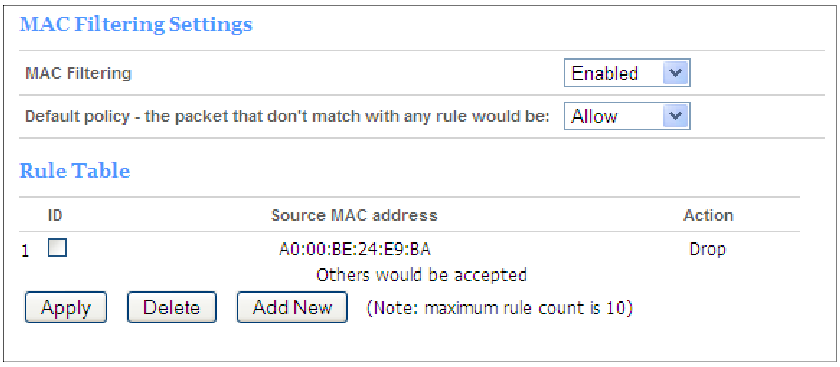
Figure4-4-2-1-2 Enable MAC Filtering function



Add Rule

Source MAC address	A0:00:BE:24:E9:BA
Action	Drop

Figure4-4-2-1-3 Add Rule



MAC Filtering Settings

MAC Filtering	Enabled
Default policy - the packet that don't match with any rule would be:	Allow

Rule Table

ID		Source MAC address	Action
1	□	A0:00:BE:24:E9:BA	Drop

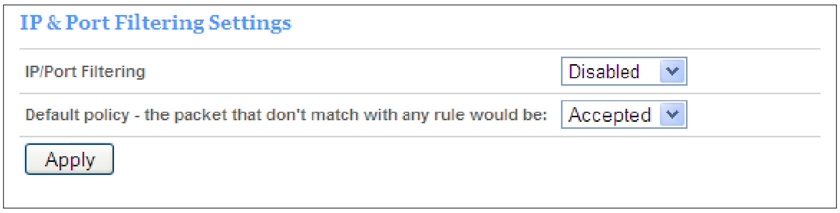
Others would be accepted

(Note: maximum rule count is 10)

Figure4-4-2-1-4 Rule Table

4.4.2.2 IP/Port Filtering

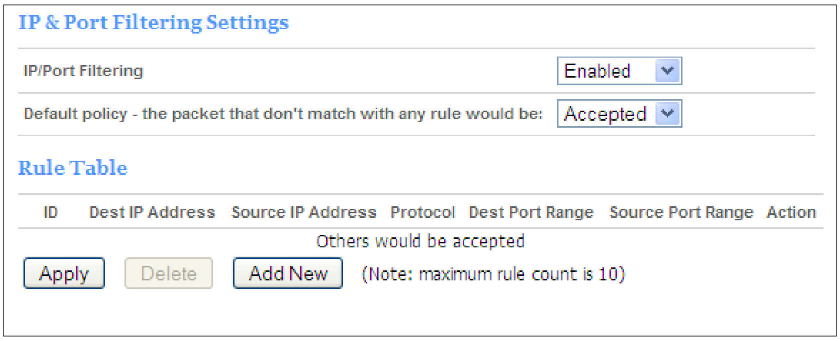
IP/Port filtering is a security tool that allows you to configure internet restrictions for specified devices based on IP addresses and port number(s). IP/Port filtering is disabled by default so it must be enabled before filters can be configured. If you choose the “Allowed” option for default policy, packets routed to the IP address specified in the rules will be dropped and vice versa. In short the “Allowed” option is creating a blacklist and the “Dropped” option is creating a whitelist.



IP & Port Filtering Settings

IP/Port Filtering	Disabled
Default policy - the packet that don't match with any rule would be:	Accepted

Figure 4-4-2-2-1 IP/Port filtering page



IP & Port Filtering Settings

IP/Port Filtering	Enabled
Default policy - the packet that don't match with any rule would be:	Accepted

Rule Table

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
Others would be accepted						

(Note: maximum rule count is 10)

Figure4-4-2-2-2 Enable IP/Port Filtering function

- **Dest IP Address**

  Enter the IP address of the IP packet destination.

- **Source IP Address**

  Enter the IP address of the IP packet source.

- **Protocol**

  Define what protocol to be filtered.

- **Dest Port Range**

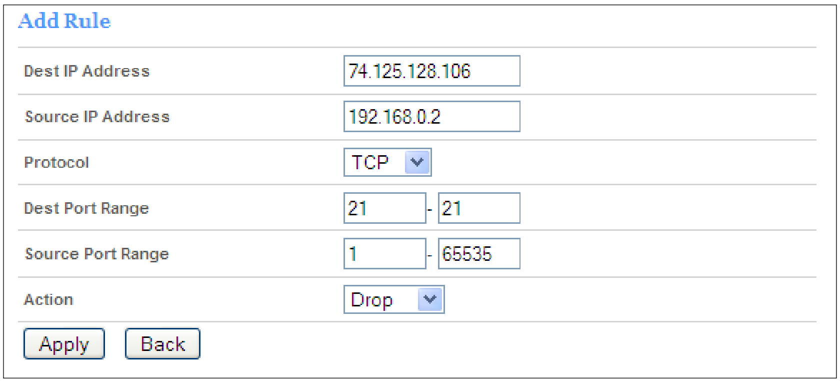
  Define port numbers to be filtered (port 80 is for http).

- **Source Port Range**

  1 - 65535

- **Action**

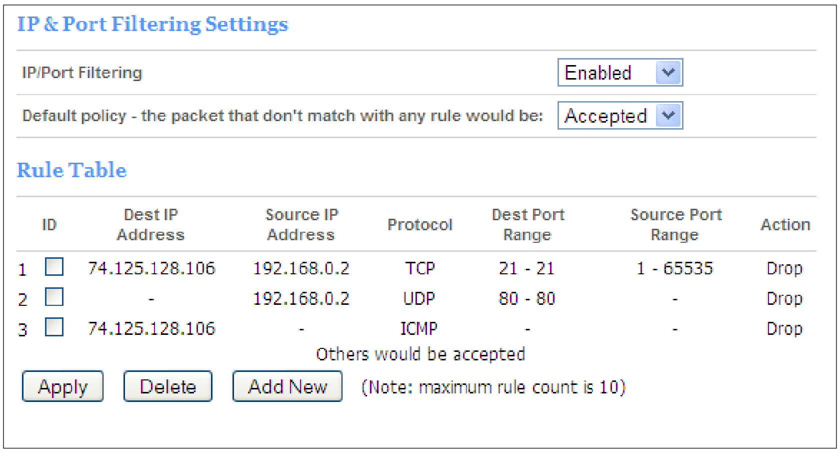
  Choose to accept or drop packets matching with the configured rules.



Add Rule

Dest IP Address	74.125.128.106
Source IP Address	192.168.0.2
Protocol	TCP
Dest Port Range	21 - 21
Source Port Range	1 - 65535
Action	Drop

Figure 4-4-2-2-3 Add New Rule



IP & Port Filtering Settings

IP/Port Filtering	Enabled
Default policy - the packet that don't match with any rule would be:	Accepted

Rule Table

ID		Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
1	□	74.125.128.106	192.168.0.2	TCP	21 - 21	1 - 65535	Drop
2	□	-	192.168.0.2	UDP	80 - 80	-	Drop
3	□	74.125.128.106	-	ICMP	-	-	Drop

Others would be accepted

(Note: maximum rule count is 10)

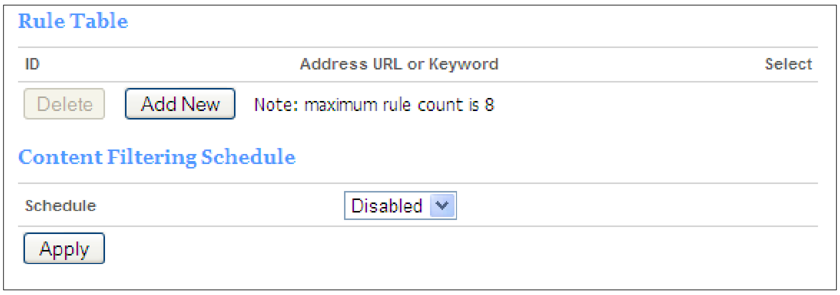
Figure 4-4-2-2-4 Rule Table

4.4.2.3 Content Filtering

On this page you can configure content filtering and the content filtering schedule.

- **Content Filtering**

Content filtering blocks all traffic to and from web browsers containing words or URL's specified in the rules.



Rule Table

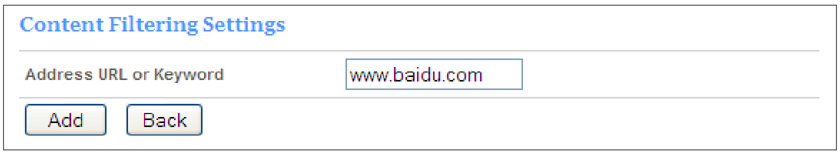
ID	Address URL or Keyword	Select

Note: maximum rule count is 8

Content Filtering Schedule

Schedule: Disabled

Figure 4-4-2-3-1 Content Filtering page



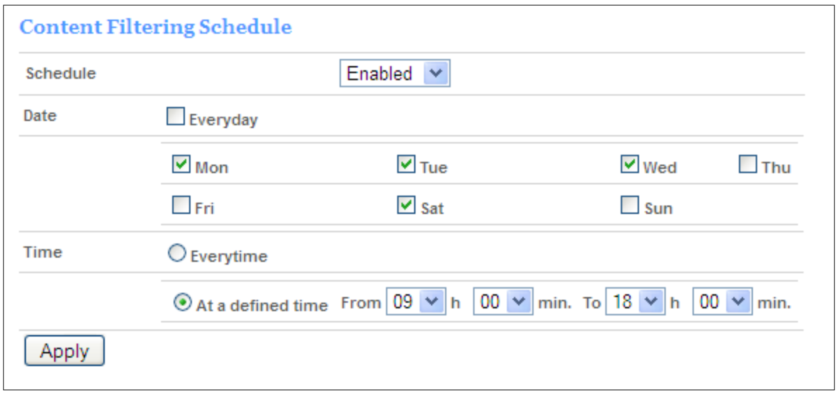
Content Filtering Settings

Address URL or Keyword: www.baidu.com

Figure 4-4-2-3-2 Add New Rule

- **Content Filtering Schedule**

Here you can configure a schedule to define when the rules should take effect. This feature is disabled by default.



Content Filtering Schedule

Schedule: Enabled

Date: □ Everyday

☑ Mon ☑ Tue ☑ Wed □ Thu

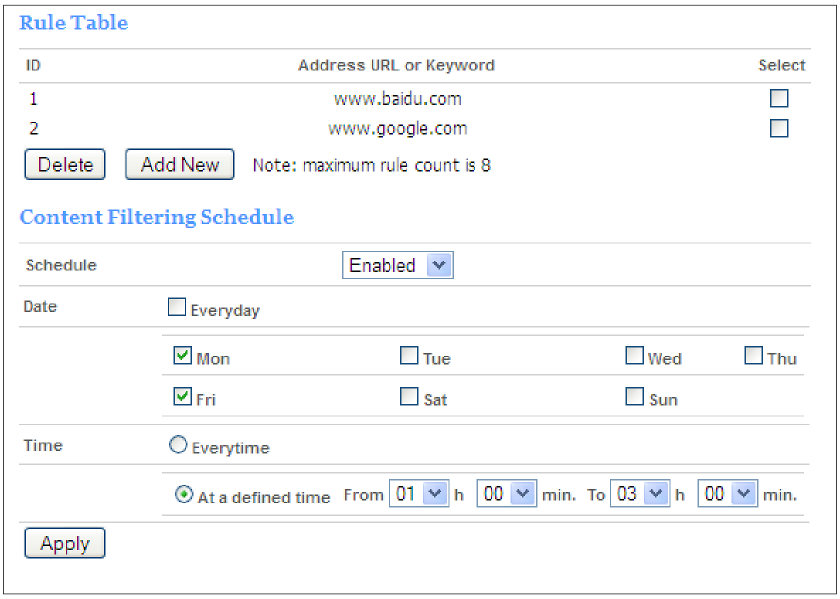
□ Fri ☑ Sat □ Sun

Time: ○ Everytime

● At a defined time From 09 h 00 min. To 18 h 00 min.

Apply

Figure 4-4-2-3-3 Configure Filtering Schedule



Rule Table

ID	Address URL or Keyword	Select
1	www.baidu.com	□
2	www.google.com	□

Delete Add New Note: maximum rule count is 8

Content Filtering Schedule

Schedule: Enabled

Date: □ Everyday

☑ Mon □ Tue □ Wed □ Thu

☑ Fri □ Sat □ Sun

Time: ○ Everytime

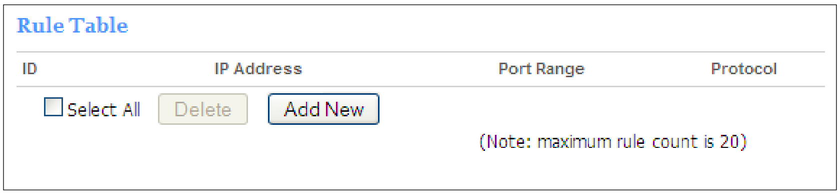
● At a defined time From 01 h 00 min. To 03 h 00 min.

Apply

Figure 4-4-2-3-4 Content Filtering Rules

4.4.2.4 Port Forwarding

By opening ports in your router traffic from the internet can be routed to a specific device and application in your LAN. This is often used by servers or devices that needs remote management



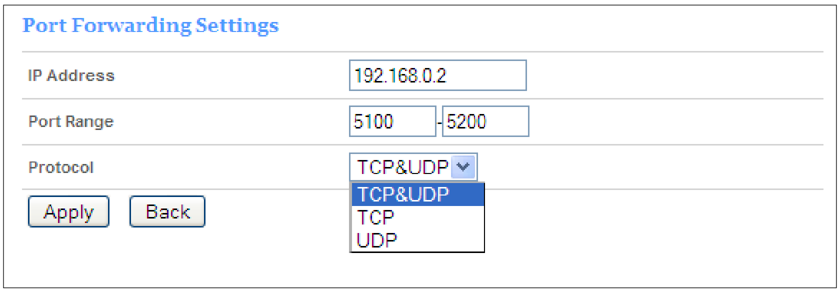
Rule Table

ID	IP Address	Port Range	Protocol

□ Select All Delete Add New

(Note: maximum rule count is 20)

Figure 3-4-2-4-1 Port Forwarding page



Port Forwarding Settings

IP Address: 192.168.0.2

Port Range: 5100 - 5200

Protocol: TCP&UDP

Figure 4-4-2-4-2 Port Forwarding Setting

- **IP Address**

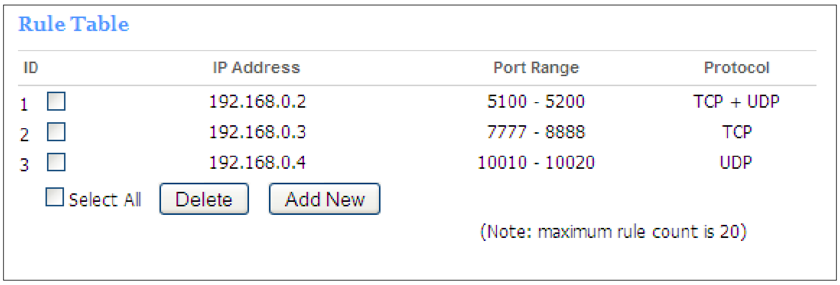
  Enter the IP address of the device in your LAN.

- **Port Range**

  Enter a fixed port number or a range of ports to be opened. This value has to match the application running on the local device (web servers often use port 80).

- **Protocol**

  Define what protocols to be allowed.



Rule Table

ID		IP Address	Port Range	Protocol
1	□	192.168.0.2	5100 - 5200	TCP + UDP
2	□	192.168.0.3	7777 - 8888	TCP
3	□	192.168.0.4	10010 - 10020	UDP

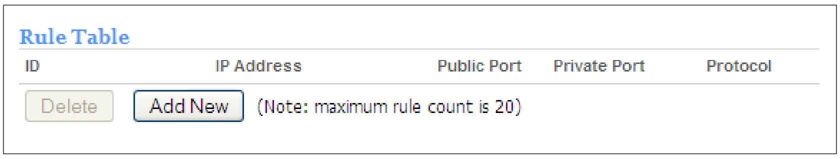
(Note: maximum rule count is 20)

Figure 4-4-2-4-3 Rule Table

4.4.2.5 Virtual Server

Virtual server is a feature similar to port forwarding. You open ports in your router to allow traffic from the internet to enter your LAN with the difference that ports can be different on the WAN and LAN side.

☞ Note: Virtual server specifies only one port and not range of ports.

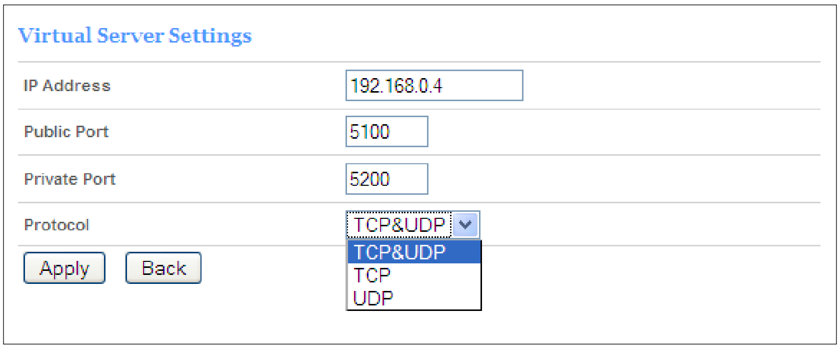


Rule Table

ID	IP Address	Public Port	Private Port	Protocol

(Note: maximum rule count is 20)

Figure 4-4-2-5-1 Virtual Server page



Virtual Server Settings

IP Address	192.168.0.4
Public Port	5100
Private Port	5200
Protocol	TCP&UDP

Figure 4-4-2-5-2 Virtual Server Setting

- **IP Address**

  Enter the IP address of the local device.

- **Public Port**

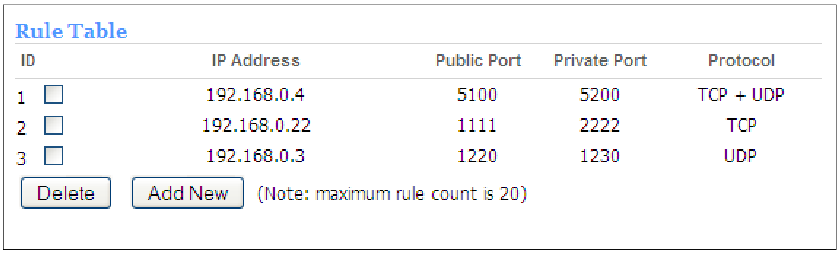
  Enter the port number to be used on the WAN side.

- **Private Port**

  Enter the port number to be used on the LAN side.

- **Protocol**

  Define what protocols to be allowed.



Rule Table

ID		IP Address	Public Port	Private Port	Protocol
1	□	192.168.0.4	5100	5200	TCP + UDP
2	□	192.168.0.22	1111	2222	TCP
3	□	192.168.0.3	1220	1230	UDP

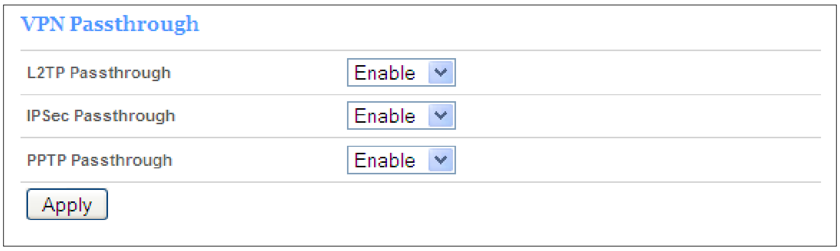
(Note: maximum rule count is 20)

Figure 4-4-2-5-3 Rule Table

4.4.2.6 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

VPN Passthrough allows VPN traffic to pass through the router. There are three main kinds of the VPN tunneling protocol, PPTP, L2TP and IPSec.



VPN Passthrough

L2TP Passthrough	Enable
IPSec Passthrough	Enable
PPTP Passthrough	Enable

Figure 4-4-2-6-1 VPN Passthrough

☞ **Note**:

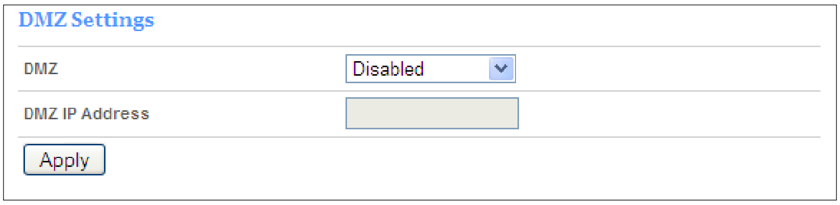
VPN Passthrough does not mean the router can create VPN endpoints. VPN pass through is a feature that allows VPN traffic created by other endpoints to "pass through" the router.

4.4.2.7 Demilitarized Zone

On this page you can configure a De-militarized Zone (DMZ) to separate internal network and Internet. By doing so all traffic destined to your WAN address will automatically be routed to the specified LAN IP address.

- **DMZ IP Address**

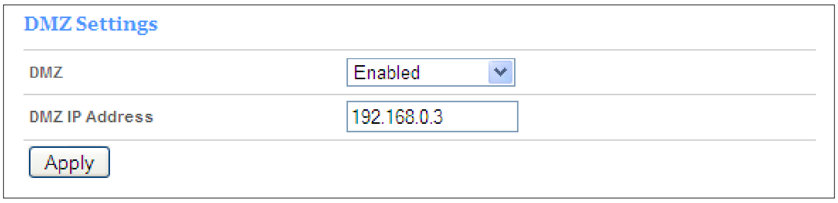
Enter the IP address of the local device.



DMZ Settings

DMZ	Disabled
DMZ IP Address	

Figure 4-4-2-7-1 DMZ page



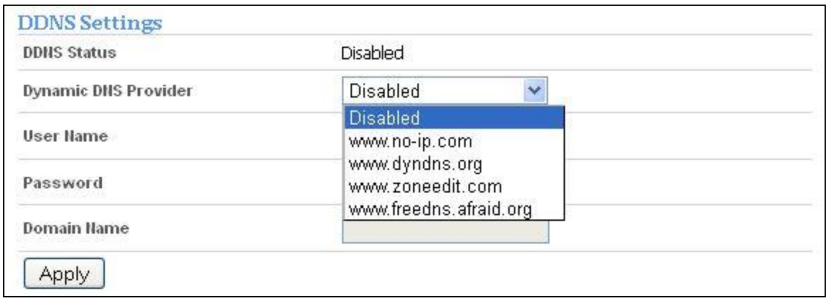
DMZ Settings

DMZ	Enabled
DMZ IP Address	192.168.0.3

Figure 4-4-2-7-2 DMZ Setting

4.4.2.8 Dynamic DNS

With DDNS you can map your WAN IP address with a DNS provided by any of the DNS providers found in the list. Dynamic DNS is disabled by default. See the chosen provider's web page for more information.



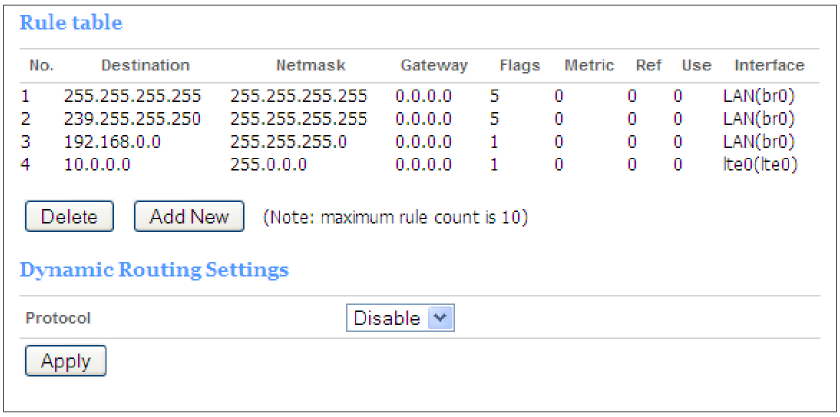
DDNS Settings

DDNS Status	Disabled
Dynamic DNS Provider	Disabled
User Name	
Password	
Domain Name	

Figure 4-4-2-8-1 Dynamic DNS setting

4.4.2.9 Routing

On this page you can add new static routes to the routing table of the router.



Rule table

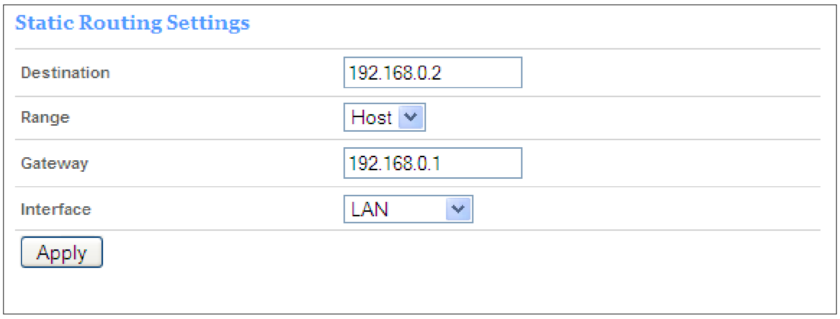
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)
4	10.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	lte0(lte0)

(Note: maximum rule count is 10)

Dynamic Routing Settings

Protocol	Disable

Figure4-4-2-9-1 Rule Table



Static Routing Settings

Destination	192.168.0.2
Range	Host
Gateway	192.168.0.1
Interface	LAN

Figure 4-4-2-9-2 Configure the static routing settings

- **Destination**

  Enter the address of the network or host to be reached from the router.

- **Range**

  Define if the destination is a host or a network.

- **Gateway**

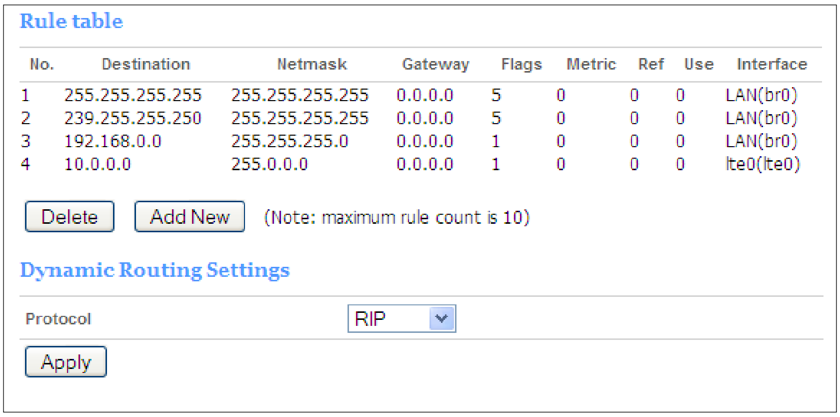
  Enter the IP address of the gateway.

- **Interface**

  Define if the gateway is on the LAN or WAN side.

- **RIP**

  When RIP is enabled the router will learn new routes from nearby devices.



Rule table

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)
4	10.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	lte0(lte0)

(Note: maximum rule count is 10)

Dynamic Routing Settings

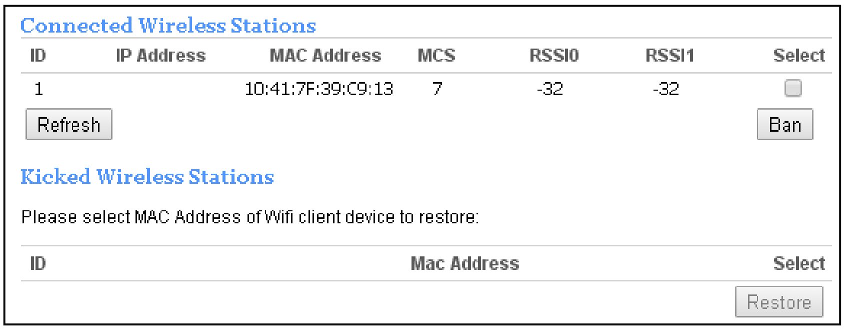
Protocol: RIP

Figure 4-4-2-9-3 New rule table

4.4.2.10 Wireless Clients

On this page you can see the detailed information about connected wireless devices, such as IP address, MAC address, MCS and RSSI. You can also ban user by selecting them by checking the box under “Select” and then click the “ban” buton, the connection will be disconnected immediately.

Banned users will be shown under kicked wireless stations. Banned users can be restored.



Connected Wireless Stations

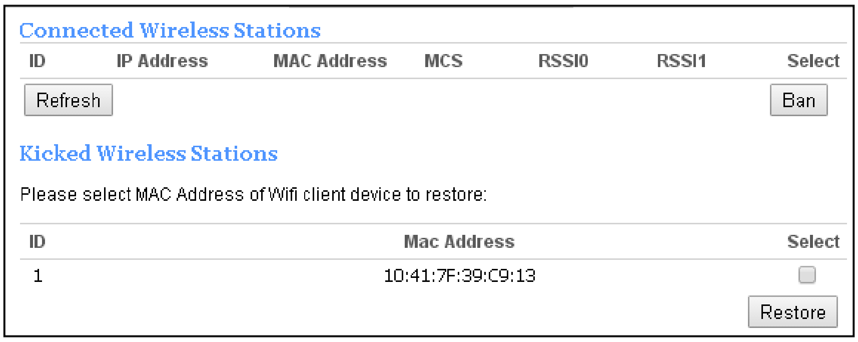
ID	IP Address	MAC Address	MCS	RSSI0	RSSI1	Select
1		10:41:7F:39:C9:13	7	-32	-32	□

Kicked Wireless Stations

Please select MAC Address of Wifi client device to restore:

ID	Mac Address	Select

Figure4-4-2-10-1 Connected Wireless Stations



Connected Wireless Stations

ID	IP Address	MAC Address	MCS	RSSI0	RSSI1	Select

Kicked Wireless Stations

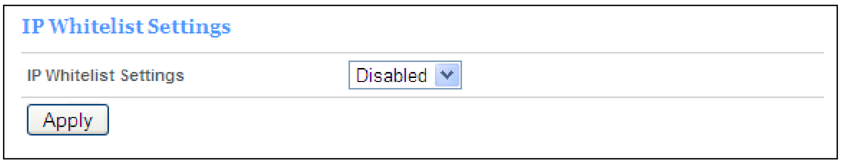
Please select MAC Address of Wifi client device to restore:

ID	Mac Address	Select
1	10:41:7F:39:C9:13	□

Figure 4-4-2-10-2 Kicked Wireless Stations

4.4.2.11 IP Whitelist

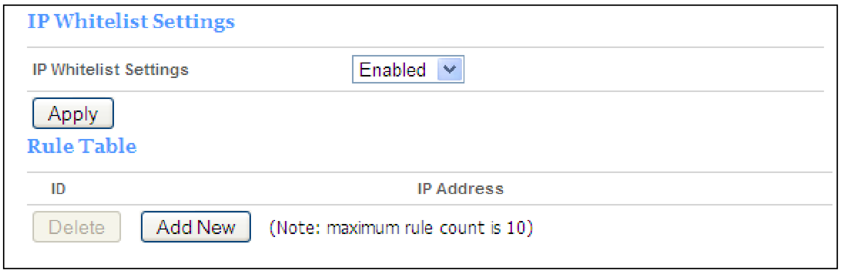
On this page you can activate IP Whitelist. When IP whitelist is active internet traffic is only permitted to devices specified in the whitelist.



IP Whitelist Settings

IP Whitelist Settings: Disabled

Figure 4-4-2-11-1 IP Whitelist page



IP Whitelist Settings

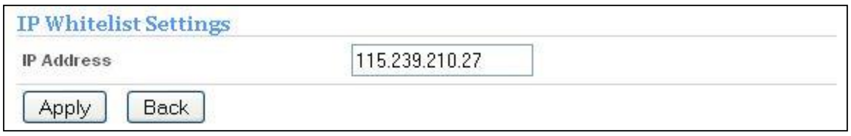
IP Whitelist Settings: Enabled

Rule Table

ID	IP Address

(Note: maximum rule count is 10)

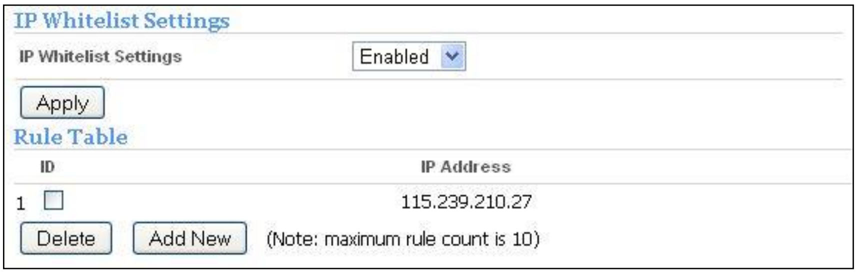
Figure 4-4-2-11-2Enable IP whitelist function



IP Whitelist Settings

IP Address: 115.239.210.27

Figure 4-4-2-11-3Add new rule



IP Whitelist Settings

IP Whitelist Settings: Enabled

Rule Table

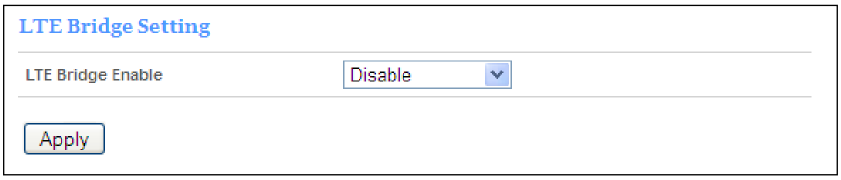
ID	IP Address
1 □	115.239.210.27

(Note: maximum rule count is 10)

Figure 4-4-2-11-4 Rule Table

4.4.2.12 Bridge Mode

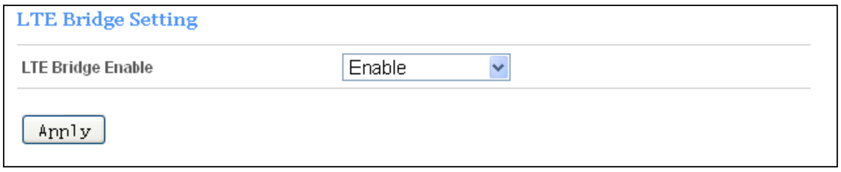
On this page you can enable bridge mode. By enabling bridge mode your WAN IP address will passed to the first device connected to the router with an Ethernet cable.



LTE Bridge Setting

LTE Bridge Enable: Disable

Figure 4-4-2-12-1 LTE Bridge Setting page

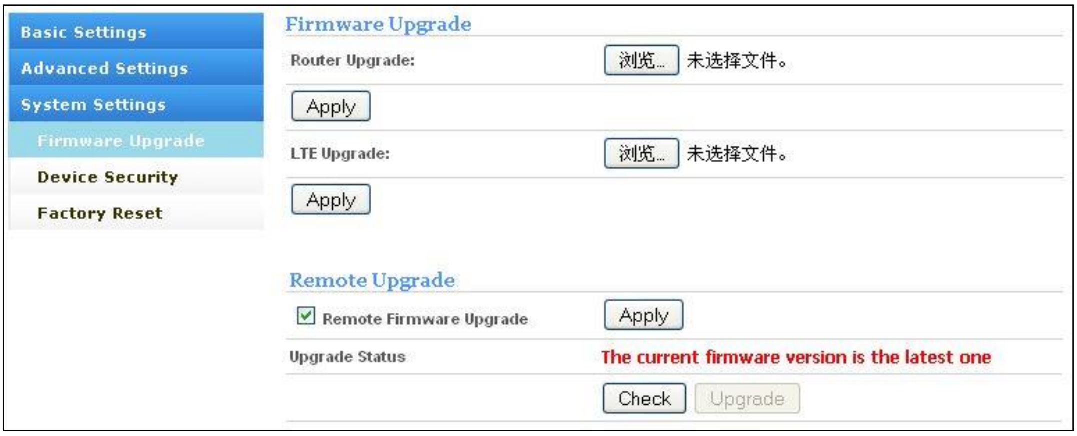


LTE Bridge Setting

LTE Bridge Enable: Enable

Figure 4-4-2-12-2Enable bridge mode

4.4.3 System Settings



Firmware Upgrade

Router Upgrade: 浏览... 未选择文件。

LTE Upgrade: 浏览... 未选择文件。

Remote Upgrade

☑ Remote Firmware Upgrade

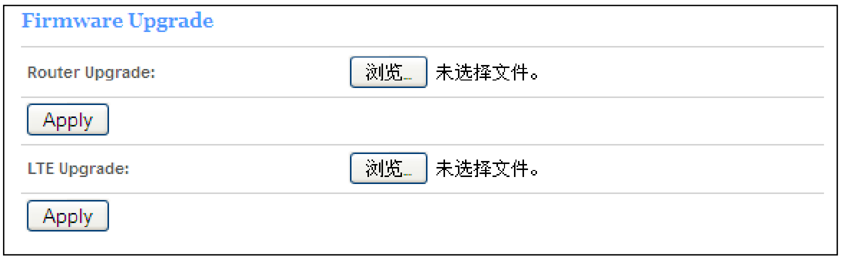
Upgrade Status: The current firmware version is the latest one

Figure 4-4-3-1 System Settings

4.4.3.1 Firmware Upgrade

- **Local Upgrade**

On this page you can upgrade both router and LTE firmware from a local device. Speak to your router supplier before performing a firmware upgrade. Any inconvenient use of this feature will damage the device.



Firmware Upgrade

Router Upgrade: 浏览… 未选择文件。

Apply

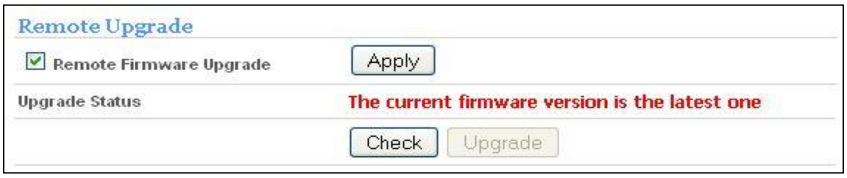
LTE Upgrade: 浏览… 未选择文件。

Apply

Figure 4-4-3-1-1 Firmware Upgrade

- **Remote Upgrade**

The remote upgrade feature will automatically scan a dedicated server for available firmware upgrades. If the device is running on battery the upgrade will be blocked if battery levels are 20% or lower. This feature can be disabled.



Remote Upgrade

☑ Remote Firmware Upgrade — Apply

Upgrade Status: The current firmware version is the latest one

Check — Upgrade

Figure 4-4-3-1-2Remote Upgrade

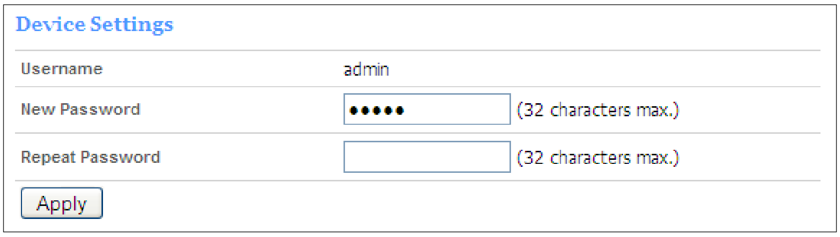
☞ **Note:**

1) The firmware version must be suitable for the corresponding hardware;
2) Please make sure the adequate and stable power supply while upgrading.

4.4.3.2 Device Security

- **Device Password**

On this page the web interface password can be changed. The password has to be between 1 and 32 characters long. When changing password you will be logged out and will have to use the new password to login again. The default password is ‘admin’.



Device Settings

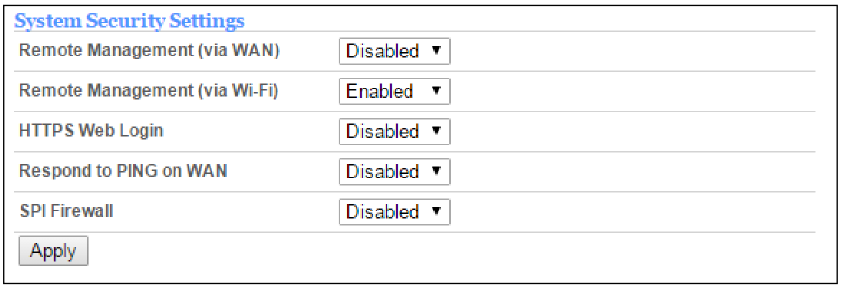
Username	admin	
New Password	●●●●●	(32 characters max.)
Repeat Password		(32 characters max.)

Apply

Figure 4-4-3-2-1 Device Settings

- **System Security Settings**

Here you can configure system security options to protect the device from the external attacks.



System Security Settings

Remote Management (via WAN)	Disabled
Remote Management (via Wi-Fi)	Enabled
HTTPS Web Login	Disabled
Respond to PING on WAN	Disabled
SPI Firewall	Disabled

Figure 4-4-3-2-2System Security Settings page

- **Remote management(via WAN)**

Enables or disables the possibility to access the web interface over the internet.

- **Remote management(via Wi-Fi)**
- Enables or disables the possibility to access the web interface over WiFI
- **HTTPS Web Login**

Enables or disables the use of https.

- **Respond to PING on WAN**

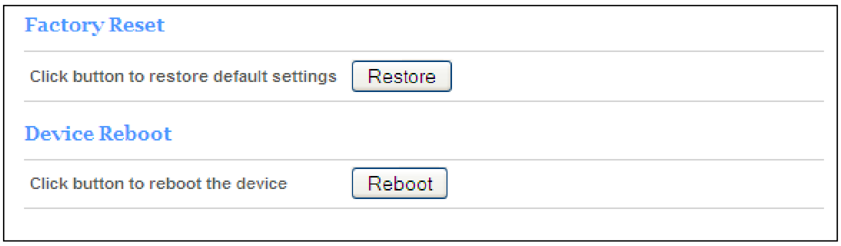
When this is enabled the router will respond on ICMP requests coming from the internet.

- **SPI Firmware**

Enable this feature to enhance protection to all the wired and wireless PCs against intruders and most known Internet attacks.

4.4.3.3 Reset& Reboot

On this page you can reboot the router or restore default settings.



Factory Reset

Click button to restore default settings

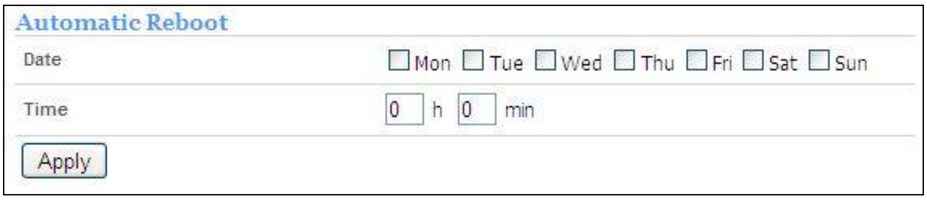
Device Reboot

Click button to reboot the device

Figure 4-4-3-3-1 Factory Reset

4.4.3.4 Scheduled Reboot

On this page you can configure the router to do scheduled reboots based on day of the week and hour of the day.


Automatic Reboot

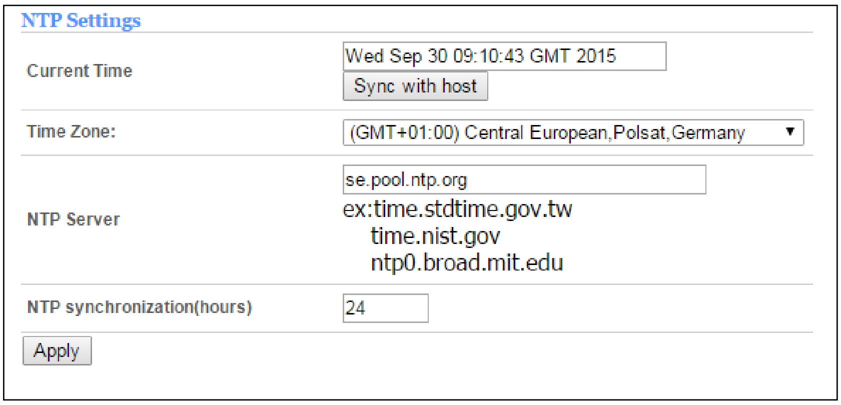
Date: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time: 0 h 0 min

Figure 4-4-3-4-1 Scheduled Reboot

4.4.3.5 NTP

On this page you can configure date and time for the router. When connected to the internet the router will automatically sync it's time settings with specified NTP server. By default it is se.pool.ntp.org.


NTP Settings

Current Time: Wed Sep 30 09:10:43 GMT 2015

Time Zone: (GMT+01:00) Central European,Polsat,Germany

NTP Server: se.pool.ntp.org

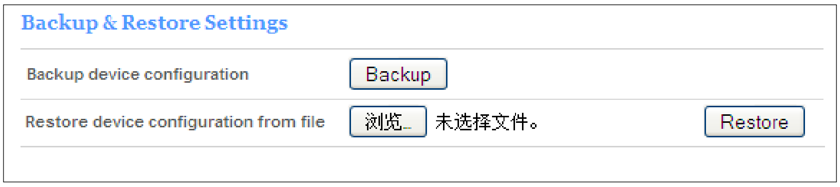
ex:time.stdtime.gov.tw
time.nist.gov
ntp0.broad.mit.edu

NTP synchronization(hours): 24

Figure 4-4-3-5-1 NTP Setting

4.4.3.6 Backup & Restore

On this page you can back up your custom configurations and store them locally in your device. The configurations-file can be used to restore your personal settings if lost or to add them on another U270V router.


Backup & Restore Settings

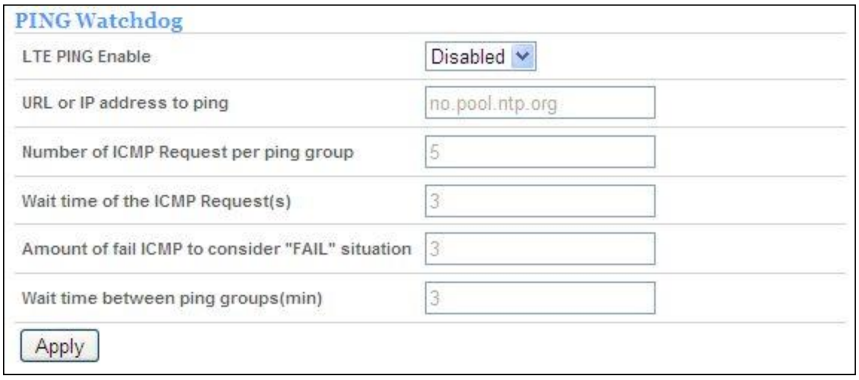
Backup device configuration

Restore device configuration from file: 未选择文件。

Figure 4-4-3-6-1 Backup & Restore

4.4.3.7 Watchdog

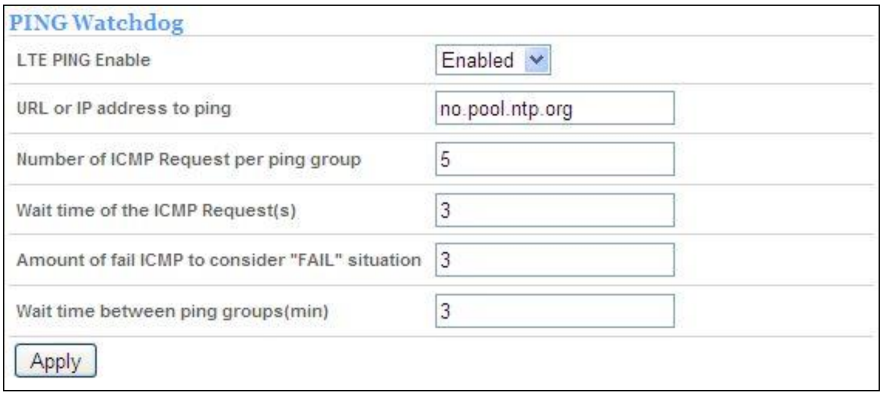
On this page you can enable the watchdog feature. The watchdog is used to ping a remote device and will reboot if a specified numbers of requests timeouts in order to rule out the router as the root cause of the failure.



PING Watchdog

LTE PING Enable	Disabled
URL or IP address to ping	no.pool.ntp.org
Number of ICMP Request per ping group	5
Wait time of the ICMP Request(s)	3
Amount of fail ICMP to consider "FAIL" situation	3
Wait time between ping groups(min)	3

Figure 4-4-3-7-1 Ping Watchdog page



PING Watchdog

LTE PING Enable	Enabled
URL or IP address to ping	no.pool.ntp.org
Number of ICMP Request per ping group	5
Wait time of the ICMP Request(s)	3
Amount of fail ICMP to consider "FAIL" situation	3
Wait time between ping groups(min)	3

Figure 4-4-3-7-2 Enable Ping Watchdog

- **URL or IP address to ping**
  Define what URL or IP to ping.

- **Number of ICMP Request per ping group**
  Define the number of ICMP requests to be sent for every ping.

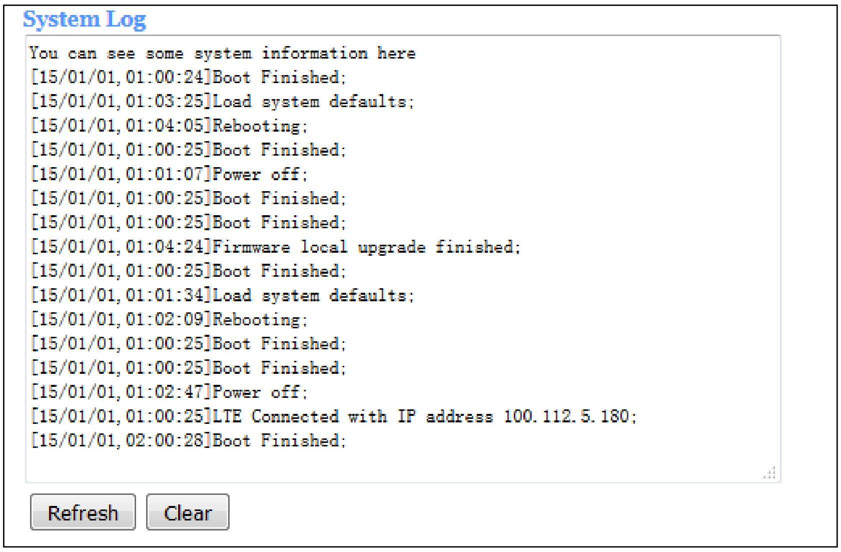
- **Wait time of the ICMP Request(s)**
  The default value is 3, you can also change it to other values.

- **Amount of fail ICMP to consider “FAIL” situation**
  Define how many timouts to be allowed per ping before restarting the router.

- **Wait time between ping groups(min):**
  Define the time in minutes between pings, the default and minimum value is 3.

4.4.3.8 System Log

In the system log you can read recent activities in the router such as IP changes, reboots and if any firmware upgrades have been made.

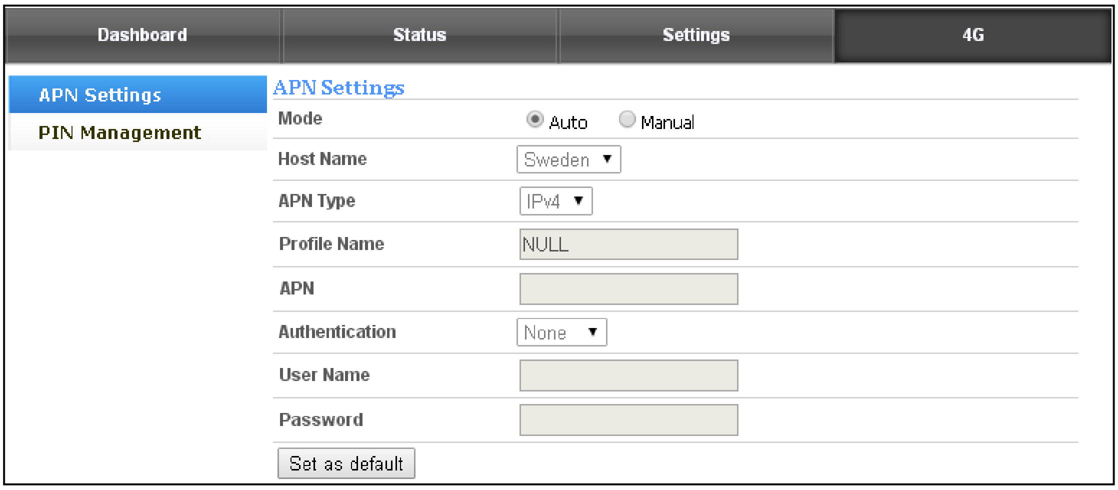

System Log

```
You can see some system information here
[15/01/01,01:00:24]Boot Finished;
[15/01/01,01:03:25]Load system defaults;
[15/01/01,01:04:05]Rebooting;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:01:07]Power off;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:04:24]Firmware local upgrade finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:01:34]Load system defaults;
[15/01/01,01:02:09]Rebooting;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:02:47]Power off;
[15/01/01,01:00:25]LTE Connected with IP address 100.112.5.180;
[15/01/01,02:00:28]Boot Finished;
```

Figure 4-4-3-8-1 System Log page

4.5 4G

The 4G section has two submenus, APN settings and PIN Management.



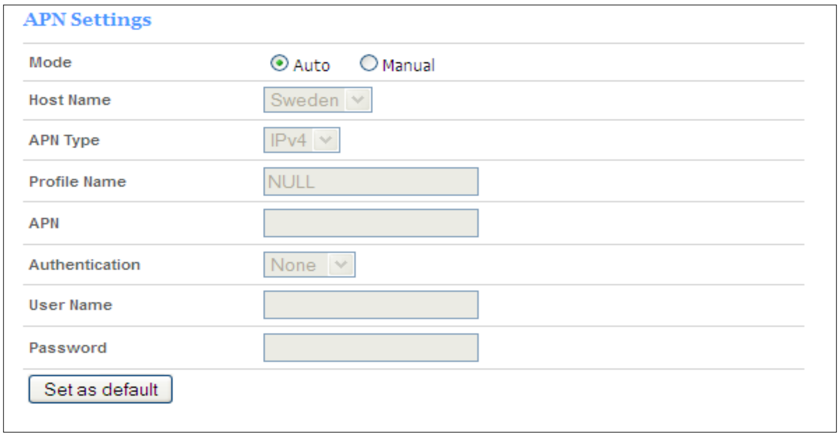
APN Settings

Mode	● Auto ○ Manual
Host Name	Sweden
APN Type	IPv4
Profile Name	NULL
APN	
Authentication	None
User Name	
Password	

Figure 4-5-1 4G

4.5.1 APN Settings

On this page you can configure the router to connect to a custom APN. Faulty configurations will make internet connection unavailable. Please contact customer service for further instructions.



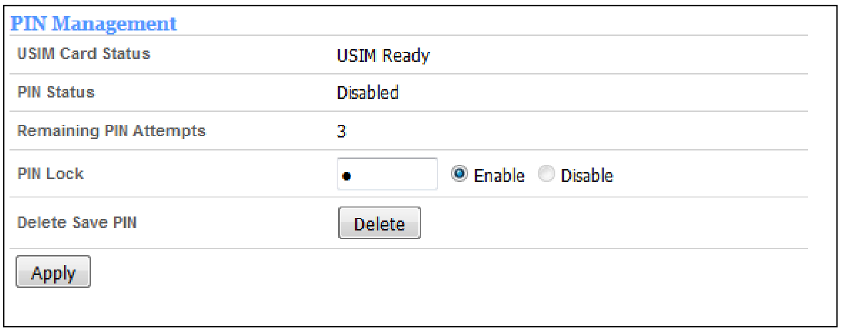
APN Settings

Mode	● Auto ○ Manual
Host Name	Sweden
APN Type	IPv4
Profile Name	NULL
APN	
Authentication	None
User Name	
Password	

Figure 4-5-1-1 LTE APN page

4.5.2 PIN Management

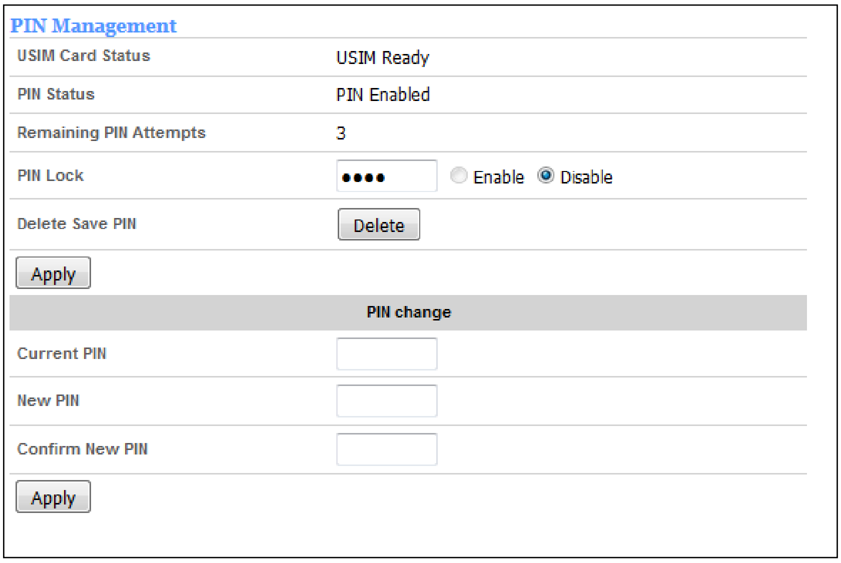
On this Page you can enable or disable the use of PIN lock. Your PIN code can be found on the back of the SIM card shipped in the router package and you will be prompted to enter it on boot. Enter the PIN by accessing the web interface page. After 3 failed attempts the device will be locked



PIN Management

USIM Card Status	USIM Ready
PIN Status	Disabled
Remaining PIN Attempts	3
PIN Lock	• ● Enable ○ Disable
Delete Save PIN	Delete

Figure 4-5-2-1 PIN Management page



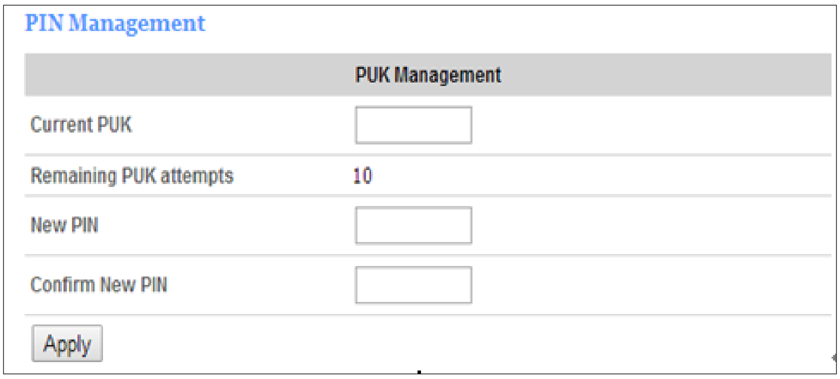
PIN Management

USIM Card Status	USIM Ready
PIN Status	PIN Enabled
Remaining PIN Attempts	3
PIN Lock	•••• ○ Enable ● Disable
Delete Save PIN	Delete

PIN change

Current PIN	
New PIN	
Confirm New PIN	

Figure 4-5-2-2 Enable the PIN



PIN Management

PUK Management	
Current PUK	
Remaining PUK attempts	10
New PIN	
Confirm New PIN	

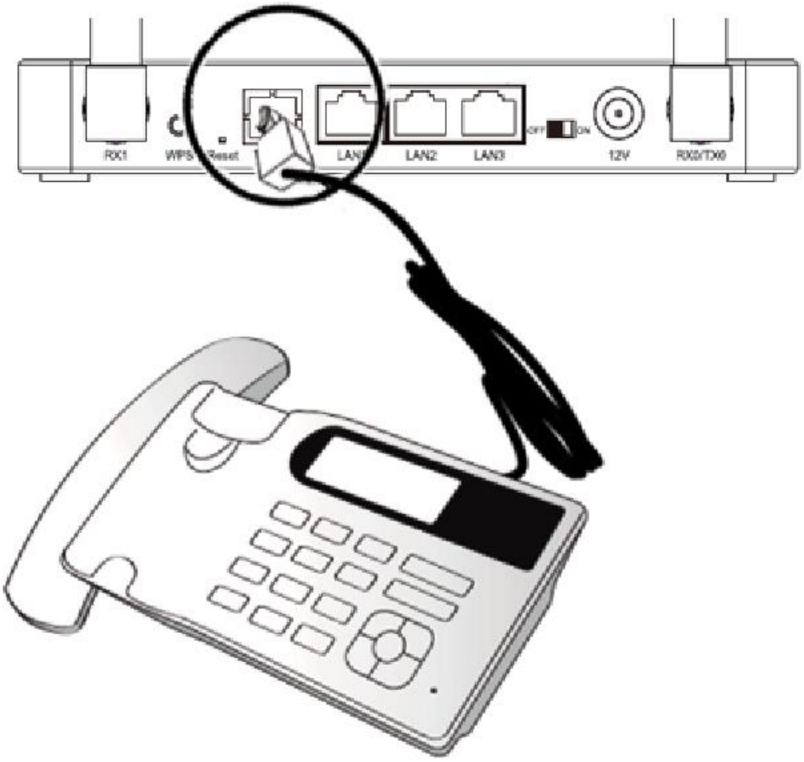
Apply

Figure 4-5-2-3 PUK Management page

5 VoIP Call Function

☞ **Note**:

Your router’s LTE and VoIP accounts must be properly activated for VoIP call functions to work. To setup your wired, landline phone for VoIP calling, plug the phone’s RJ-11 cable into the “TEL” port on your router as shown below. Consequently, you must first disconnect the phone from the fixed phone line, and connect it to the router instead.



5.1 Activating Voice over IP

In order to use Voice over IP you must have an account with Net1. If you do not have the service pleasecontact Customer Service.

5.2 Placing Voice Calls

1. Turn on the router.
2. Lift the handset from your phone.
3. When you hear a dial tone, use the phone's numeric keypad to dial the desired phone number

5.3 Receiving Voice Calls

The telephone(s) connected to the router will ring when receiving an incoming call.

1. Lift the telephone's handset to answer a call.

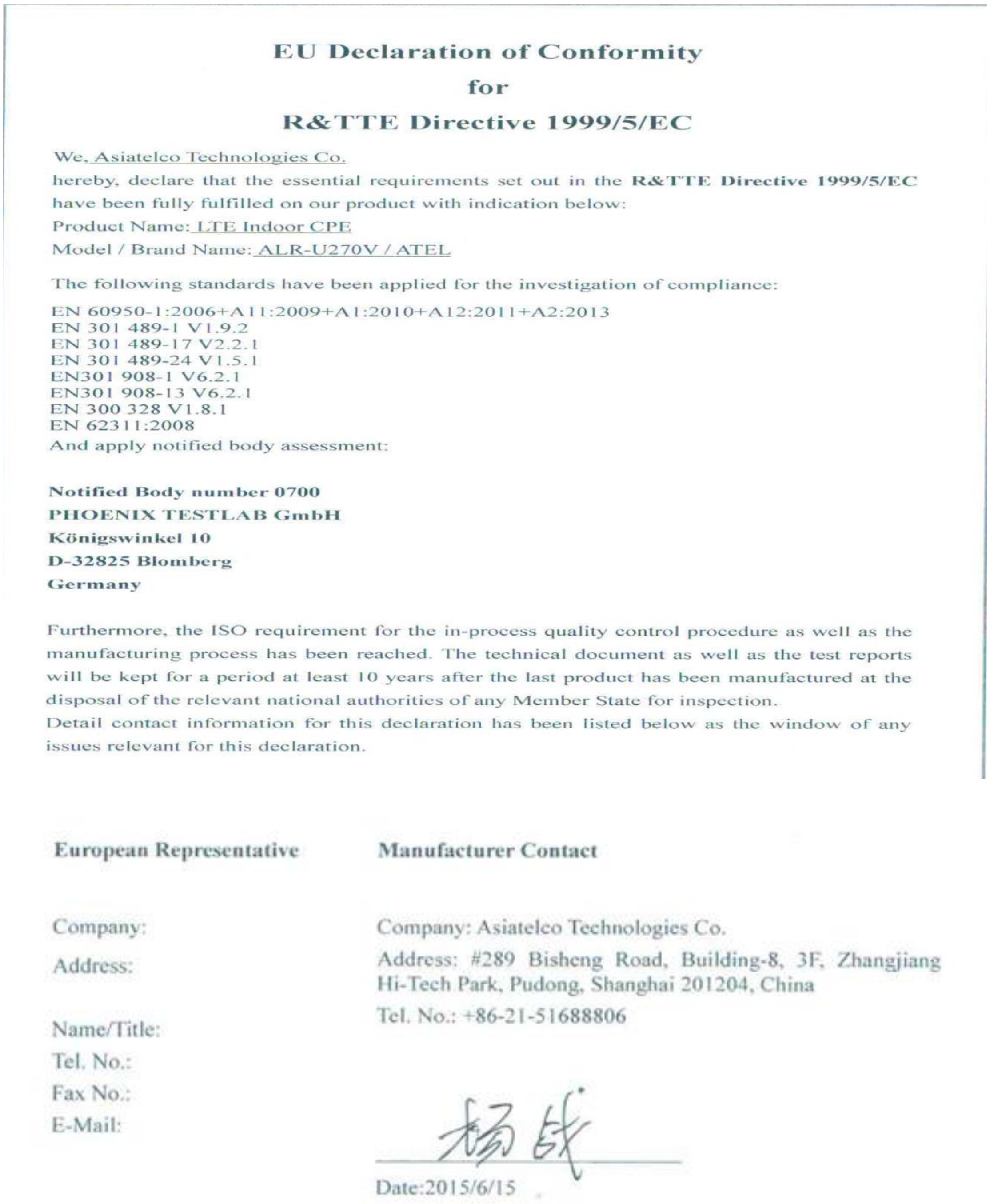
☞ **Note:**

To answer an incoming call while you are holding the receiver, press any key on the phone's numeric keypad.

6 Technical Specification

Size	180(L)*128(W)*23(H) mm
Weight	310g
Battery Type	Li-ion (2 cell), 3.7V(Max 4.2V)/5200mA/h
Operating Temperature	-20o C ~ +70o C
Storage Temperature	-30o C ~ +80o C
Humidity	5 ~ 95%
Stand by Time	Up to 7 hours
Usage Time	Up to 3 hours
Adaptor Input	AC 100-300V
Adaptor Output	12V/1A

7 Certification



EU Declaration of Conformity
for
R&TTE Directive 1999/5/EC

We, Asiatelco Technologies Co.
hereby, declare that the essential requirements set out in the **R&TTE Directive 1999/5/EC** have been fully fulfilled on our product with indication below:
Product Name: LTE Indoor CPE
Model / Brand Name: ALR-U270V / ATEL

The following standards have been applied for the investigation of compliance:

EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
EN 301 489-1 V1.9.2
EN 301 489-17 V2.2.1
EN 301 489-24 V1.5.1
EN301 908-1 V6.2.1
EN301 908-13 V6.2.1
EN 300 328 V1.8.1
EN 62311:2008
And apply notified body assessment:

Notified Body number 0700
PHOENIX TESTLAB GmbH
Königswinkel 10
D-32825 Blomberg
Germany

Furthermore, the ISO requirement for the in-process quality control procedure as well as the manufacturing process has been reached. The technical document as well as the test reports will be kept for a period at least 10 years after the last product has been manufactured at the disposal of the relevant national authorities of any Member State for inspection.
Detail contact information for this declaration has been listed below as the window of any issues relevant for this declaration.

European Representative	**Manufacturer Contact**
Company:	Company: Asiatelco Technologies Co.
Address:	Address: #289 Bisheng Road, Building-8, 3F, Zhangjiang Hi-Tech Park, Pudong, Shanghai 201204, China
	Tel. No.: +86-21-51688806
Name/Title:	
Tel. No.:	
Fax No.:	
E-Mail:	杨战
	Date:2015/6/15